CyberSource®
the power of payment

2013 Online Fraud Report

Online Payment Fraud Trends, Merchant Practices, and Benchmarks

14TH ANNUAL EDITION

CyberSource, an industry leader in fraud management solutions, enables businesses to continually improve profitability by detecting fraud sooner and more accurately and by streamlining fraud management operations. CyberSource provides a complete range of solutions, including training, consultation, active management of fraud screening, and outsourcing all or part of your fraud management operations.

CyberSource sponsors these annual online surveys to support the industry in preventing and managing online payment fraud by sharing fraud management best practices and benchmarks.

GET TAILORED VIEWS OF FRAUD MANAGEMENT PIPELINE METRICS

To get a view customized for your company's size and industry, please contact CyberSource at 1.888.330.2300 or online at **www.cybersource.com/contact_us**.

For additional information, whitepapers and webinars, or sales assistance:

- **Fraud Management Solutions:** http://www.cybersource.com/products_and_services/fraud_management/
- **Resource Center:** http://www.cybersource.com/cgi-bin/resource_center/resources.cgi

© 2013 CyberSource Corporation, a Visa company. All rights reserved.

TABLE OF CONTENTS

© 2013 CyberSource Corporation, a Visa company. All rights reserved.

EXECUTIVE SUMMARY

To better understand the impact of payment fraud for companies selling online, CyberSource sponsors annual surveys addressing the detection, prevention and management of online payment fraud. This report summarizes findings from our 14th annual survey.*

ESTIMATED $3.5 BILLION LOST TO ONLINE FRAUD

In 2012, companies reported losing an average of 0.9% of total online revenue to fraud, similar to 2010 levels. Using 2012 industry market projections on eCommerce sales in North America[1], we estimate that total revenue loss translates to approximately $3.5 billion. Because the size of the overall market has grown, the revenue loss equates to $100,000,000 more versus 2011.

Although the fraud rate by revenue has gone down, the fraud rate by order increased from 0.6% in 2011 to 0.8% in 2012. The average ticket value for a fraudulent order was $200, approximately 1/3 higher than a valid order ($149).

For the 54% of survey respondents that accept international orders, the fraud rate for orders outside of North America was twice as high – 1.6%. With international sales comprising 14% of overall orders (and even more so for the largest companies), fraud management mitigation strategies will need to be closely monitored and scrutinized.

CHALLENGES MANAGING GROWTH PERSIST

2013 eCommerce sales are projected to grow at 12%[2], yet some organizations may be unable to fully capitalize on these opportunities. 77% of survey participants indicated that both fraud staffing levels and budgets would remain the same or lower. With eCommerce sales increasing, and 1 out of 4 orders manually reviewed, companies will be challenged to screen more orders with the same resources and budget.

*Note: this report provides benchmarks on total fraud rates (chargebacks and credits issued directly to consumers by companies). As such, these metrics tend to be higher than those reported by banks and card schemes, which generally base reported rates on chargeback activity only.

[1] Based on eMarketer projections, with a 13% uplift to account for industry segments covered by the survey but not by eMarketer's market sizing.

[2] eMarketer

© 2013 CyberSource Corporation, a Visa company. All rights reserved.

FOCUS ON OPERATIONAL EFFICIENCY

Of the orders manually reviewed, 75% are ultimately accepted, and one could ask why the orders were sent to review to begin with. Two factors may be at work. First, automated fraud screening strategies may need fine-tuning to screen more orders. Second, some companies send even slightly suspicious orders to review for further scrutiny, fearing customer insult if the order was rejected outright.

However, for the 60% of respondents that track fraud rate after manual review, the fraud rate by order was 4%, ***5 times higher*** than the average. The high post-review order acceptance rate could be driven by company policy around customer experience or not having more confidence in their analysis to reject the order. Regardless, a closer look at the factors driving high post-review order acceptance is warranted.

ON THE RADAR: MOBILE

In 2012, mobile commerce sales were estimated to be $24.7 billion, an increase of 82% over 2011[3]. However, mobile commerce is the least likely channel to be evaluated for payment fraud, in comparison to MOTO or eCommerce. The good news is that nearly 30% of respondents track mobile commerce fraud, which is a marked improvement over 2011 (8%), and highlights increasing awareness and the growing importance of mobile commerce. The bad news: the mobile channel shows the highest revenue fraud loss rate, at 1.4%. As mobile sales continue to rise rapidly, companies will need to adjust their fraud management strategies accordingly.

FULL PROCESS VIEW

How can organizations achieve and sustain an acceptable fraud level while maintaining a positive customer experience and keeping overhead costs in line? How can organizations achieve this balance, especially in the face of ever-changing fraud threats?

To address this, a full view of the fraud management process is required. Using the framework outlined in the graphic on page 6, companies can assess their performance in key areas of their fraud screening operations: automated screening (data, detectors, risk models, rules), manual review, order dispositioning (accept/reject decisions), and fraud claim management. Once a performance baseline has been established, companies can then analyze and tune their operations to optimize outcomes. This report details key metrics and practices at each point in the process to provide you with benchmarks and best practice insights. Custom views of these benchmarks and practices are available through CyberSource – see front page for contact information.

[3] eMarketer

PROFIT LEAKS

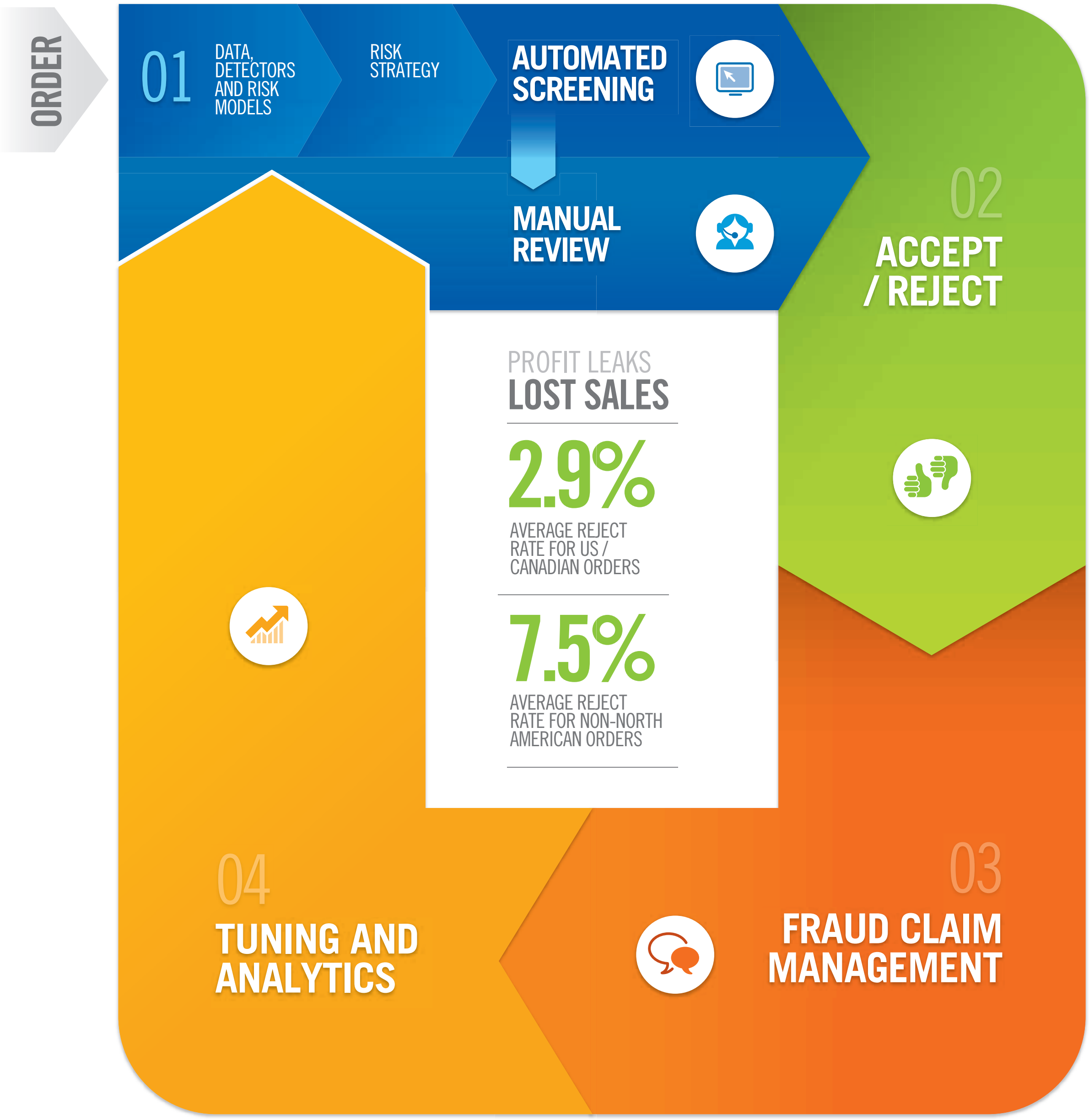
STAFFING & SCALABILITY

73% MERCHANTS REVIEW ORDERS

52% OF FRAUD MANAGEMENT BUDGET IS SPENT ON REVIEW STAFF COSTS

69% NO PLANS TO CHANGE STAFFING LEVELS IN 2013

□ □ ■ □ ON AVERAGE 1 OUT OF 4 ORDERS ARE REVIEWED



PROFIT LEAKS

LOST SALES

2.9% AVERAGE REJECT RATE FOR US / CANADIAN ORDERS

7.5% AVERAGE REJECT RATE FOR NON-NORTH AMERICAN ORDERS

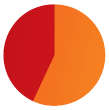
PROFIT LEAKS

FRAUD LOSS & ADMINISTRATION

$3.5B ESTIMATED LOST TO ONLINE PAYMENT FRAUD

0.9% AVERAGE FRAUD RATE BY REVENUE

0.8% AVERAGE FRAUD RATE BY ORDER

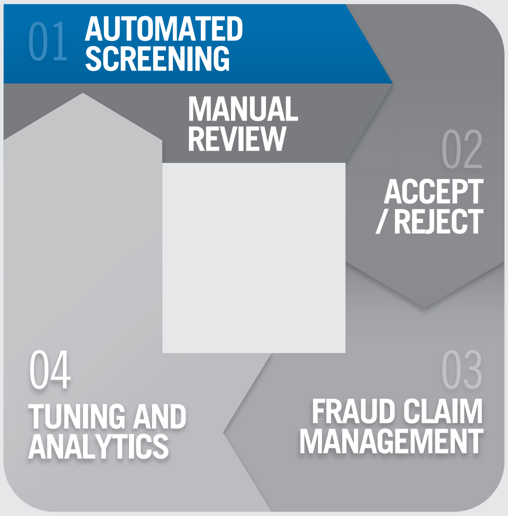


43% FROM CHARGE-BACKS

57% FROM CREDITS ISSUED

© 2013 CyberSource Corporation, a Visa company. All rights reserved.

AUTOMATED SCREENING



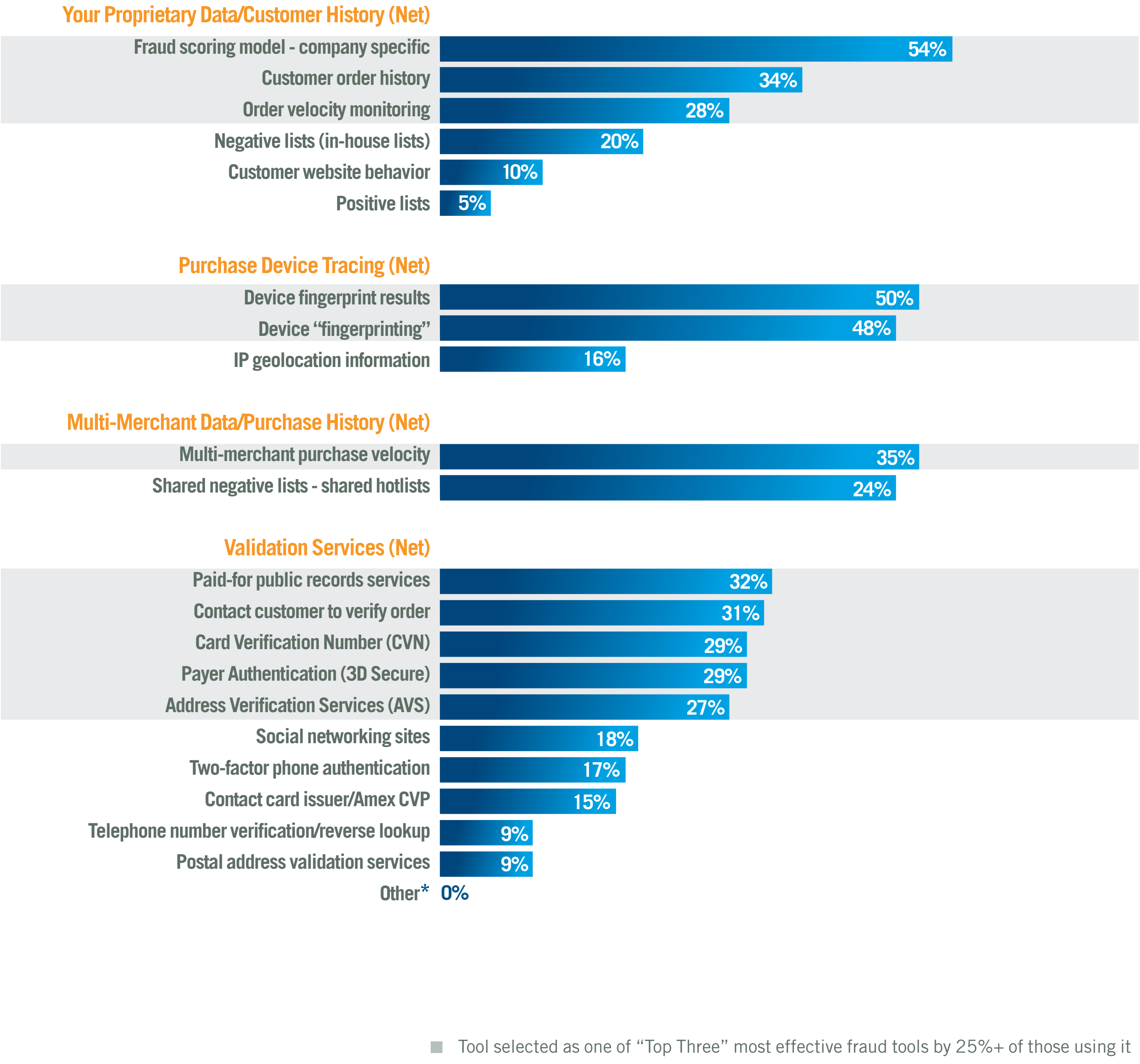
In this stage, orders typically go through an automated screening process, in which a rules-based system and/or risk evaluation is applied to determine the likelihood of fraud. The objective is to have the automated system handle most of the decisions, leaving only the most suspicious orders for the review team to investigate. This provides for faster, more accurate and efficient screening of orders.

Ideally, automated order screening should leverage the organization's own data, third-party fraud prevention tools (such as IP geolocation, device fingerprinting, fraud-scoring calculation models, multi-merchant data, velocity checks, and more), as well as a variety of services made available by the various card schemes (i.e., Card Verification Value 2, Verified by Visa, etc.). In 2012, organizations reported using an average of 4.9 tools overall, the same as in 2011.

The chart on page 8 highlights the fraud tools that were deemed most effective by organizations, looking at both automated and manual screening. Similar to 2011, company-specific fraud scoring models and device fingerprinting continue to be cited as one of the top three most effective tools.

© 2013 CyberSource Corporation, a Visa company. All rights reserved.

MOST EFFECTIVE FRAUD MANAGEMENT TOOLS



*Other – No respondents selected out-of-wallet/in-wallet challenge, credit history check, biometric indicators and Google Maps as top three most effective tools.
Base: Merchants with annual eCommerce sales ≥$25M who use tool: automated or manual (excludes None / No Answer).

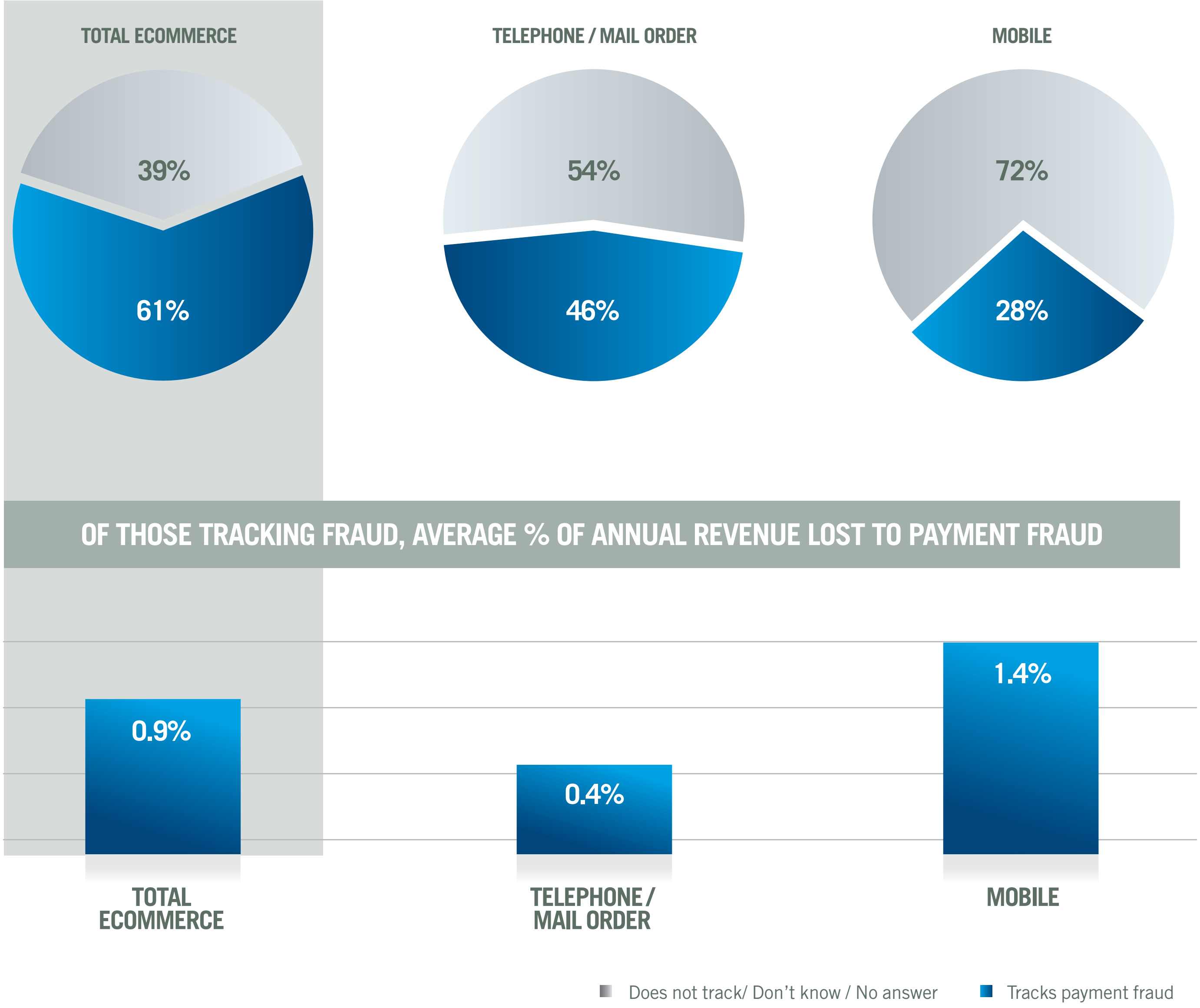
© 2013 CyberSource Corporation, a Visa company. All rights reserved.

SPOTLIGHT ON MOBILE

With smartphones and tablets now outpacing PC/laptop sales[4], 40% of respondents state that they have mobile commerce sales (in comparison to 33% in 2011, an increase of 20%). As a result of significantly more mobile devices, more companies are beginning to track payment fraud in mobile commerce – 28%, in comparison to 8% reported in 2011.

The mobile channel poses tremendous opportunity for companies, but also poses some risk, as typical validation tools available through the web are not as effective for mobile. On the other hand, mobile phones provide rich data to companies to validate the consumer, especially through a mobile app.

FRAUD RATE BY REVENUE, PER SALES CHANNEL



[4] http://mashable.com/2012/02/03/smartphone-sales-overtake-pcs/

© 2013 CyberSource Corporation, a Visa company. All rights reserved.

MOBILE FRAUD MITIGATION STRATEGIES

SOURCE: AARIJ KHAN, SENIOR DIRECTOR PRODUCT MARKETING, THREATMETRIX

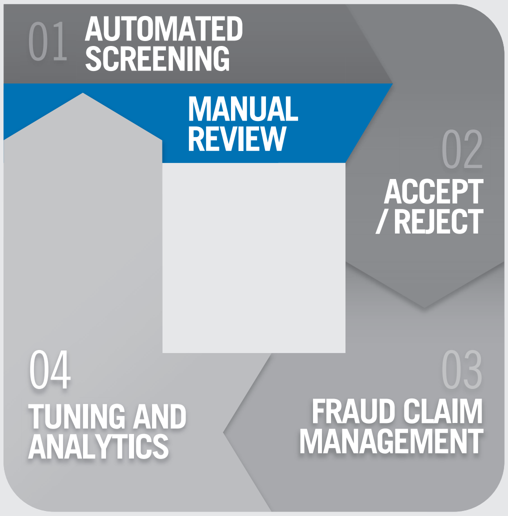
Closely monitor and track behavior from transactions that come from mobile devices and cross-check against other historical data. If a customer uses an app to purchase, you can potentially obtain additional information to use in your screening rules.

Factor the presence of malware and other unauthorized software running on the mobile device into your fraud screening strategies. Mobile malware, like PC malware, can steal account credentials, take over sessions, perform injection attacks and corrupt browsers and apps engaged in logins and transactions.

Utilize and create rules around device fingerprinting, proxy piercing and VPN detection. For example, with iOS, Android, and Windows 8 devices, fraudsters can bypass the pre-installed browser and use one that they've downloaded instead, enabling them to create proxy sites that mask their actual location. Similarly, free VPN solutions enable fraudsters to select an originating IP address. As VPN solutions are often customized, traditional detection routines do not work as efficiently.

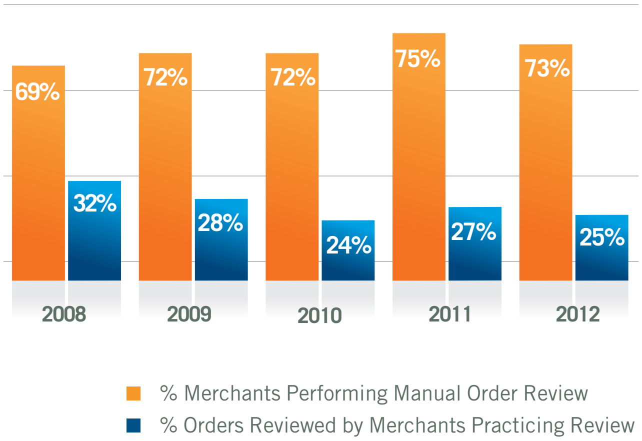
If you have a dedicated mobile app, promote its use to your customers. Apps can provide much better separation on the device (sandboxing) and stronger OS-level protection.

MANUAL REVIEW



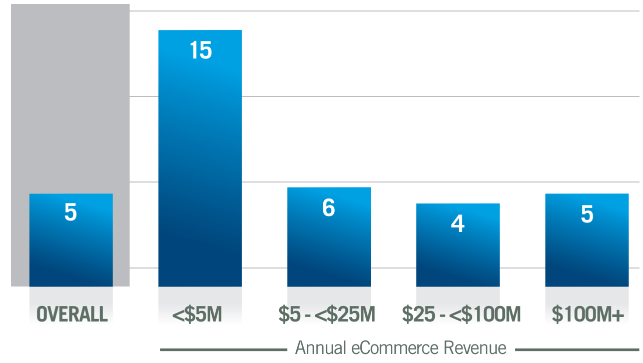
After an evaluation by an automated screening process, orders with more ambiguous transaction characteristics will be sent to manual review for a deeper level of investigation. In this process, an individual or team of reviewers will use additional data verification sources accompanied by their judgment (developed through experience) to render a decision. For maximum efficiency, in addition to consolidating various external verification sources into one, compact user interface, the review team should have access to a case management system to optimally distribute or allocate orders in queue(s).

MANUAL REVIEW TRENDS



MINUTES TO RESEARCH AND ACCEPT/REJECT SUSPICIOUS ORDERS

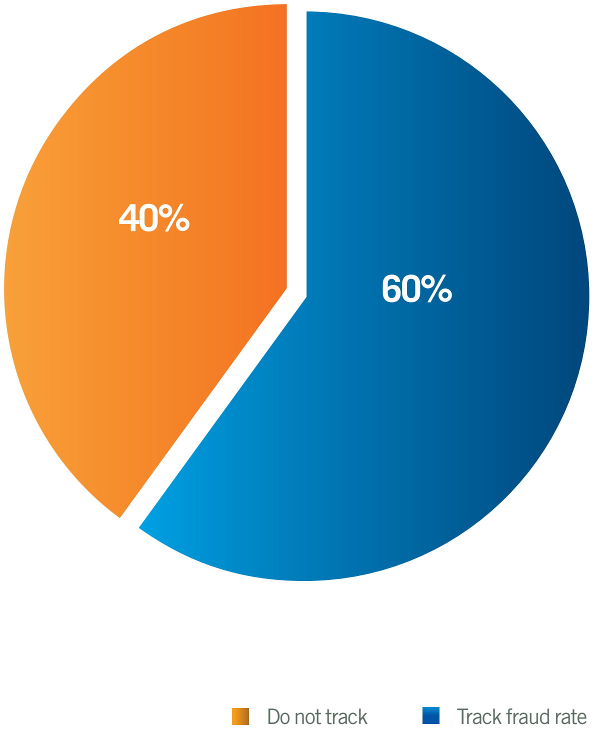
(OVERALL AND BY MERCHANT SIZE)



% who take 20+ minutes	20%	41%	17%	10%	6%

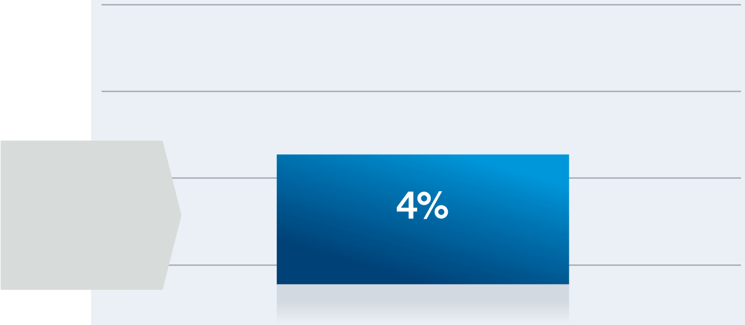
© 2013 CyberSource Corporation, a Visa company. All rights reserved.

% OF RESPONDENTS THAT TRACK FRAUD FOR MANUALLY REVIEWED ORDERS



Base: Merchants practicing manual review (excludes Don't know/ No answer)

% OF MANUALLY ACCEPTED ORDERS THAT TURNED OUT TO BE FRAUDULENT - 2012



Base: Merchants with annual eCommerce sales ≥$25M practicing manual review (excludes Don't know/ No answer)

© 2013 CyberSource Corporation, a Visa company. All rights reserved.

OPTIMIZING MANUAL REVIEW SUCCESS: MEASURE, REFINE, MEASURE, REFINE….

CARL TUCKER, PRINCIPAL, CYBERSOURCE GLOBAL SERVICES

Because review teams typically account for the largest cost in an organization's fraud management budget, monitoring and optimizing review team performance is critical. Consider how the team is performing in the context of your operational goals and helping to meet your company's overall financial objectives.

1. Balance effectiveness with efficiency by measuring key performance metrics by reviewer and review team:

   - Chargebacks in total, as a percentage of the number of orders and total transaction revenue

   - Average and aggregate review times to disposition orders

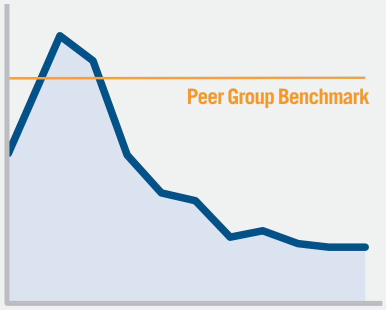
   - Number of transactions reviewed

   - (if possible) Number of inadvertent customer insults (false positives)

2. Measure these overall fraud management KPIs over a specific period of time to determine trends and areas of concern and areas of improvement. Establish a baseline for comparison, using your historical data and/or industry benchmarks (such as those provided by CyberSource – see sample charts on the right).

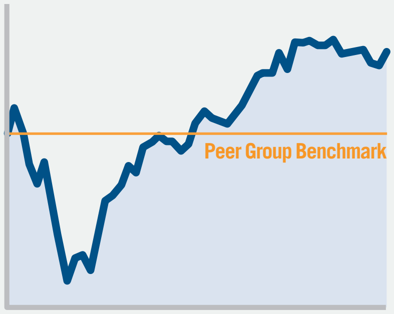
FRAUD RATE %

October 2011-September 2012



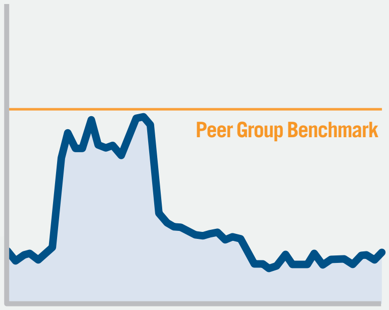
APPROVAL RATE %

October 2011-September 2012



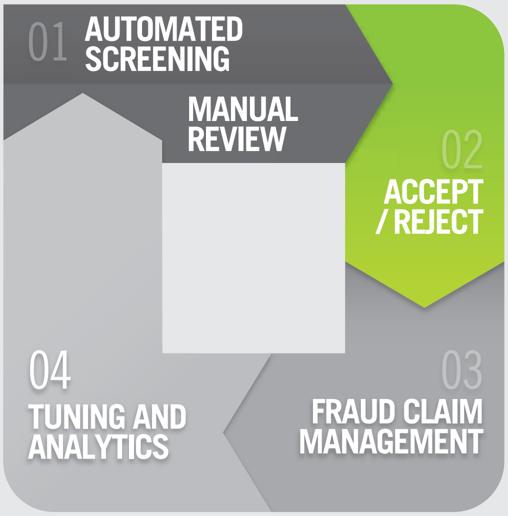
MANUAL REVIEW RATE %

October 2011-September 2012



© 2013 CyberSource Corporation, a Visa company. All rights reserved.

ORDER DISPOSITIONING (ACCEPT/REJECT)

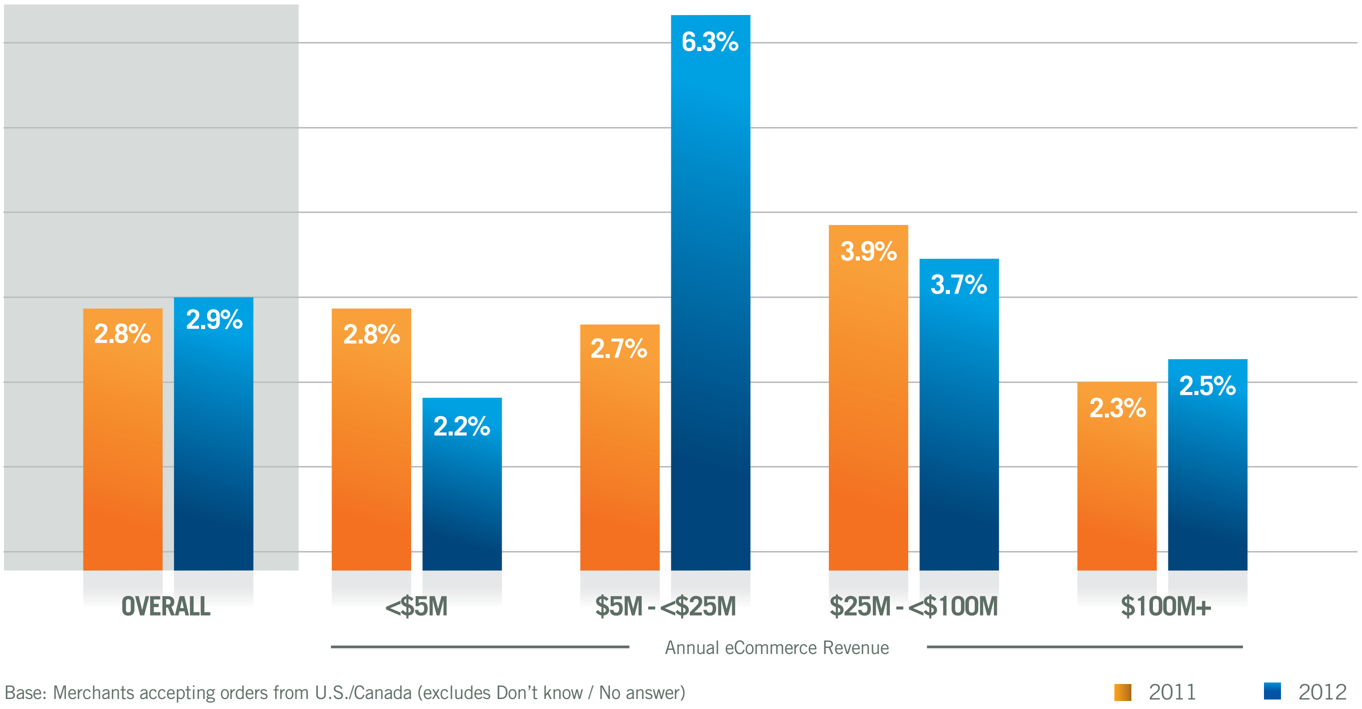


The ultimate outcome of an automated and manual review process is the decision to either Accept or Reject an order. As a general rule of thumb, an equivalent number of orders should be accepted as rejected. Excessively high or low post-manual review acceptance rates after manual review can indicate that more orders than necessary are being diverted to manual review, which increases overhead costs and delays in fulfilling customer orders. This skewing of manual Accept-Reject rates can typically be resolved by tuning the automated fraud detection system earlier in the process to bring the manual review rates into better balance.

© 2013 CyberSource Corporation, a Visa company. All rights reserved.

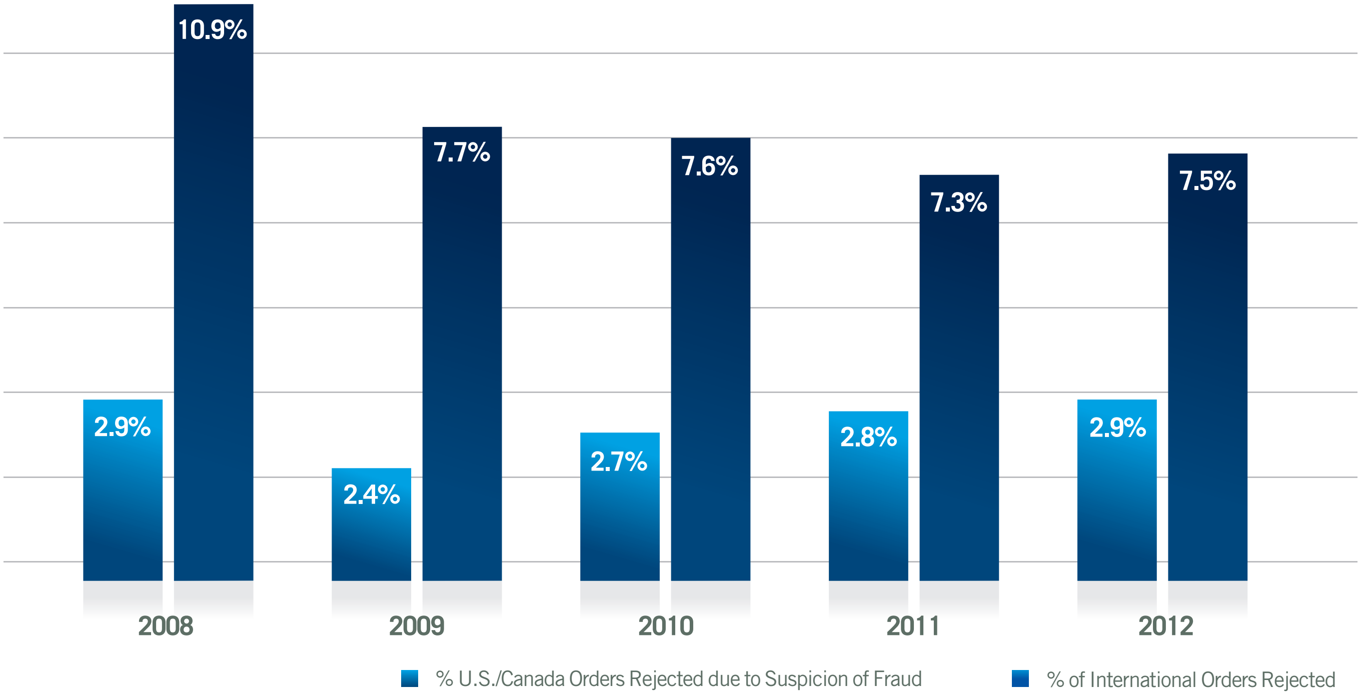
AVERAGE % ORDERS REJECTED DUE TO SUSPICION OF FRAUD

(OVERALL AND BY MERCHANT SIZE)



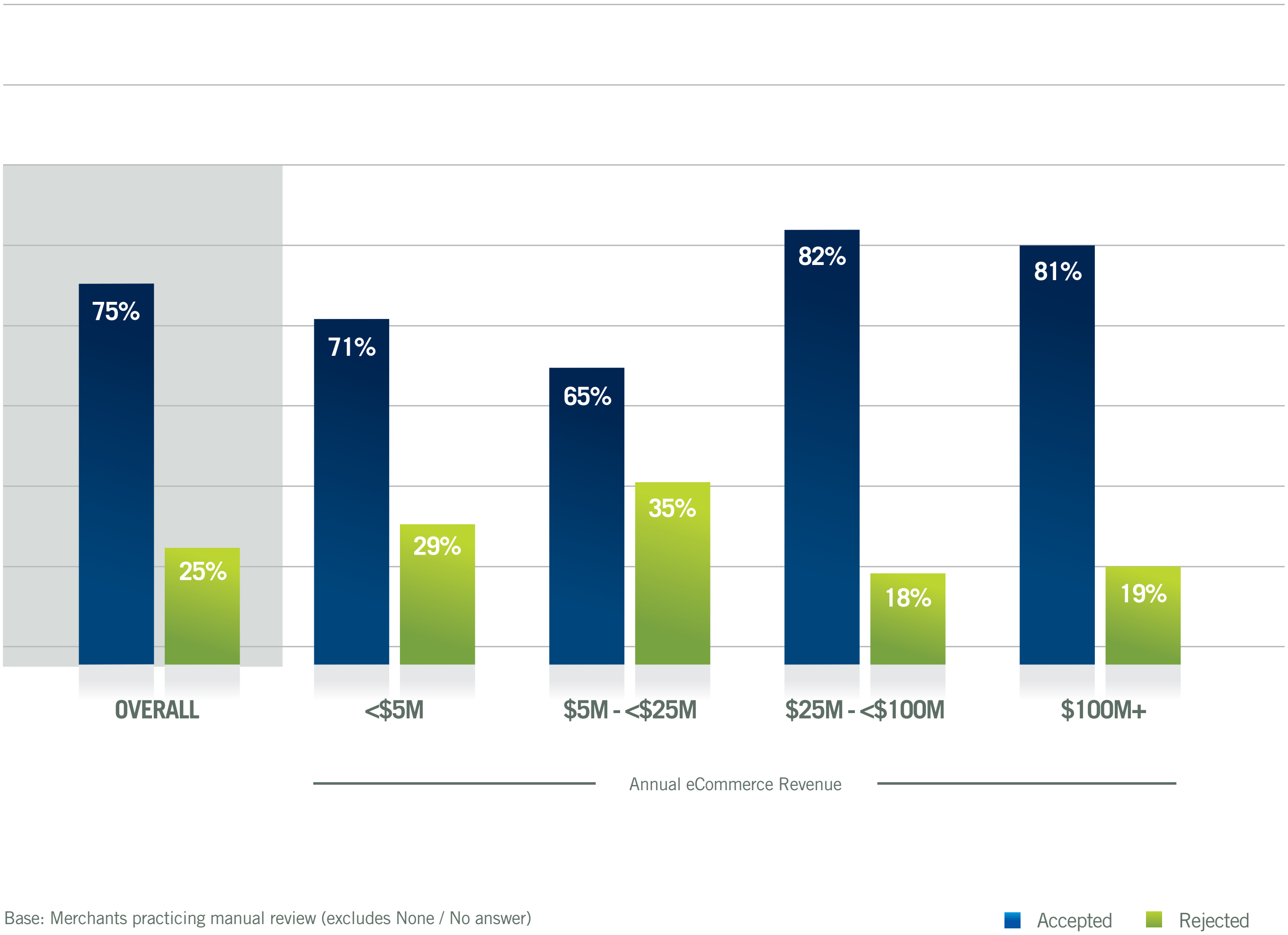
Base: Merchants accepting orders from U.S./Canada (excludes Don't know / No answer)

ORDER REJECTION RATES, DOMESTIC VS. INTERNATIONAL



© 2013 CyberSource Corporation, a Visa company. All rights reserved.

POST-REVIEW ORDER ACCEPTANCE RATE
(OVERALL AND BY MERCHANT SIZE) - 2012



Base: Merchants practicing manual review (excludes None / No answer)

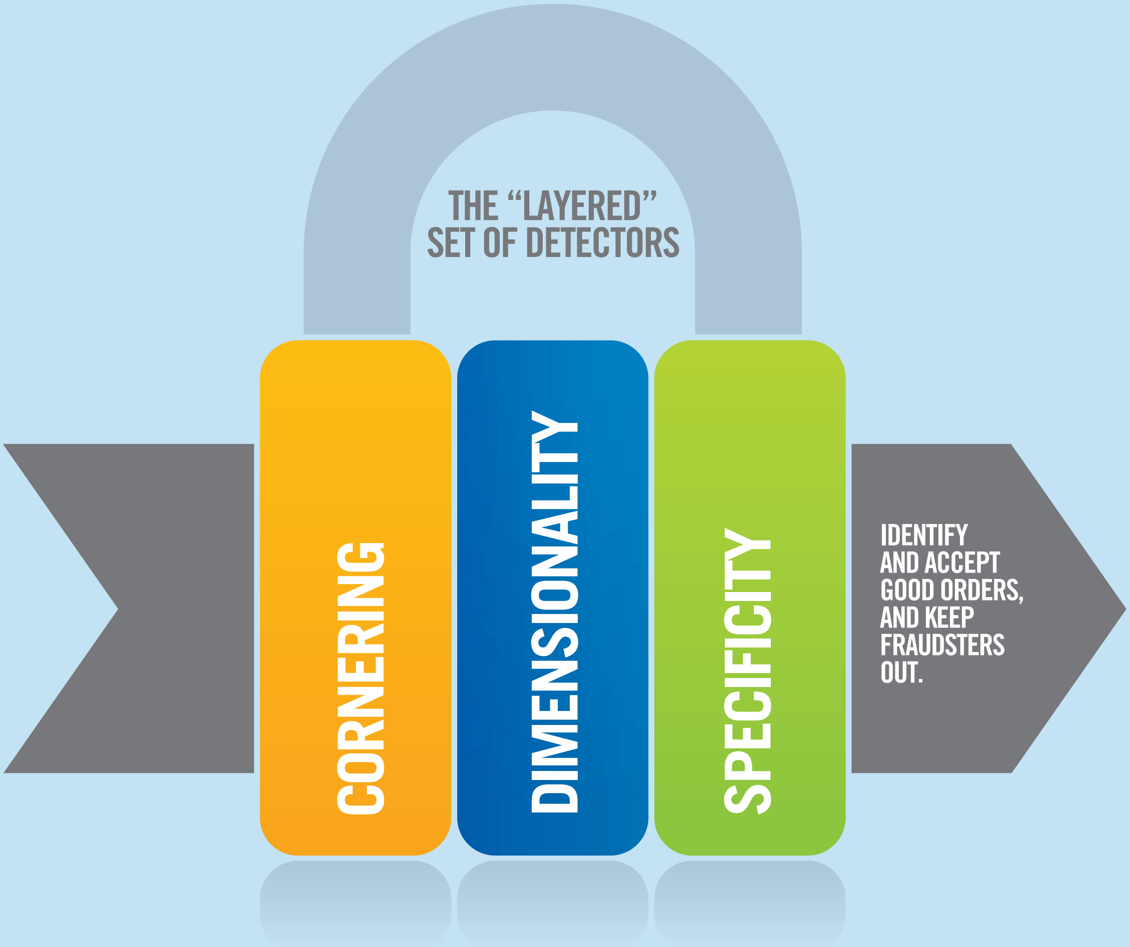
© 2013 CyberSource Corporation, a Visa company. All rights reserved.

CREATING LAYERS TO DEFEND AGAINST FRAUD

SCOTT BODING, BUSINESS LEADER IN RISK SOLUTIONS, CYBERSOURCE

The goal of any fraud management strategy is to accurately identify and accept good orders, while keeping fraudsters out.

We advocate a multi-factored approach or using a "layered" set of detectors in concert, including techniques shown here.


THE "LAYERED" SET OF DETECTORS
CORNERING
DIMENSIONALITY
SPECIFICITY
IDENTIFY AND ACCEPT GOOD ORDERS, AND KEEP FRAUDSTERS OUT.

ASK FOR RELIABLE INFORMATION

Force the fraudster to surrender a key piece of reliable information using hard rules (e.g., disable shipping redirect and require that the shipping address is deliverable).

ADD DIMENSIONS OF RELATED DATA

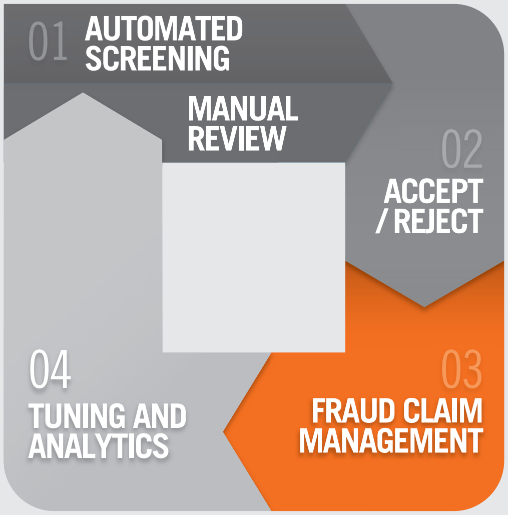
Once you have the key piece of reliable information, add "dimensions" of other, related data that you have on the order (e.g., device fingerprint, account number, email, etc.), then build rules using these dimensions in combination. For example, create rules with shipping address + velocity intervals AND shipping address + account number(s). It makes it more difficult to perpetrate fraud systematically.

CREATE A SAFETY NET

In the absence of reliable or available data, use "generic" information to create a safety net and assess risk based on the level of information you have. For instance, if shipping address information is not available, create rules around risk levels associated with the zip code or country of the shipping address.

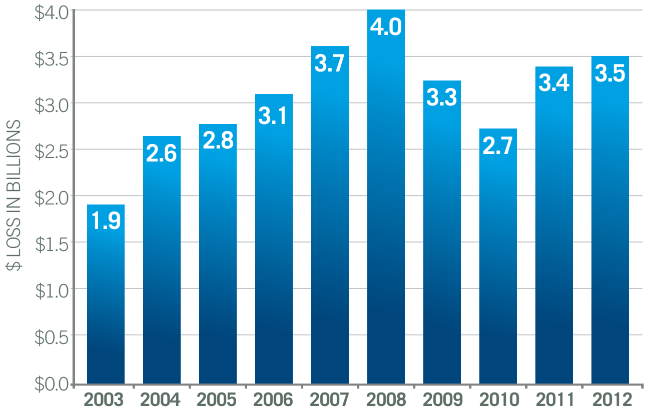
© 2013 CyberSource Corporation, a Visa company. All rights reserved.

FRAUD CLAIM MANAGEMENT

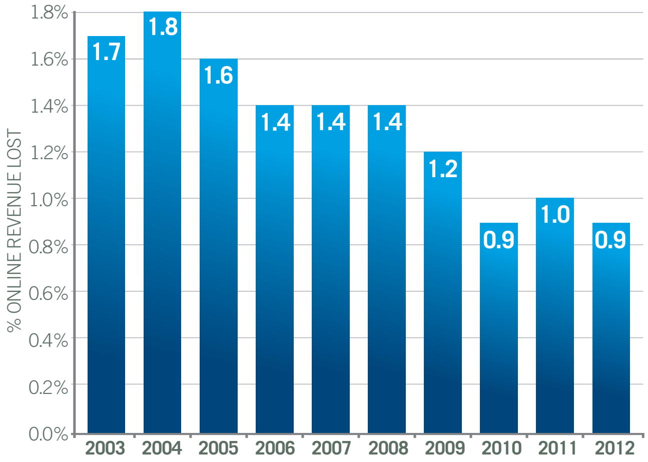


We define fraud as chargebacks and credits issued by the merchant due to likelihood of fraud. As a result, actual fraud rates reported tend to be higher than those cited by banks or card schemes. When monitoring the level and trend of fraud loss, we focus on fraud rate by revenue (also known as the revenue fraud loss rate), fraud rate by order (fraudulent order rate), and the average value of a fraudulent order relative to a valid order. In 2012, the average ticket value for a fraudulent order was 35% higher than a valid order ($200 versus $149, respectively).

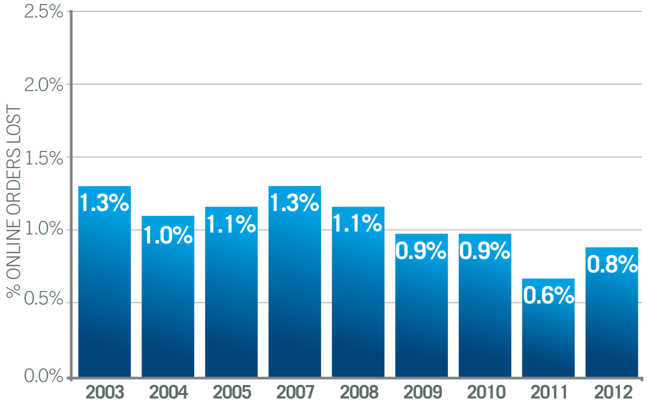
ESTIMATED REVENUE LOST DUE TO ONLINE FRAUD



AVERAGE FRAUD RATE BY REVENUE



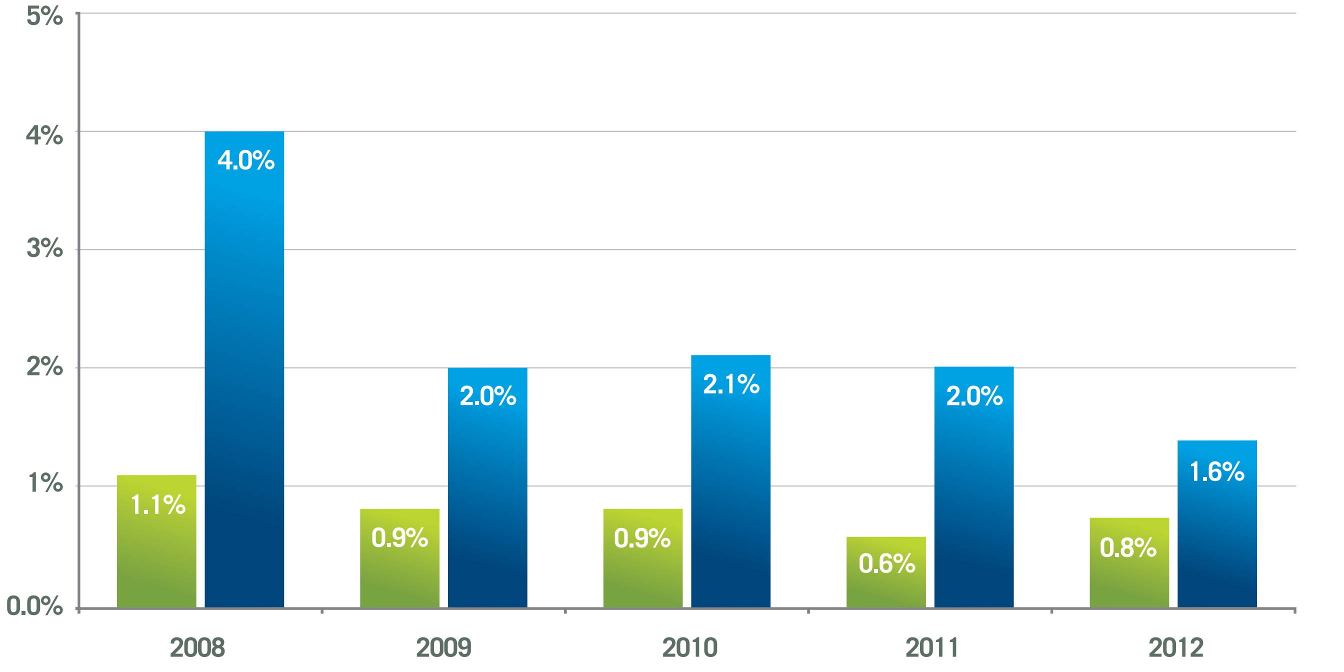
AVERAGE FRAUD RATE BY ORDER



© 2013 CyberSource Corporation, a Visa company. All rights reserved.

Although the domestic fraudulent order rate has increased to 0.8%, the international fraudulent order rate has decreased to 1.6%. However, it's still twice as high.

FRAUD RATE BY ORDER, DOMESTIC VS. INTERNATIONAL



*Base: Merchants accepting orders from U.S./Canada (excludes Don't know / No answer)
**Base: Merchants accepting international orders (excludes Don't know / No answer)

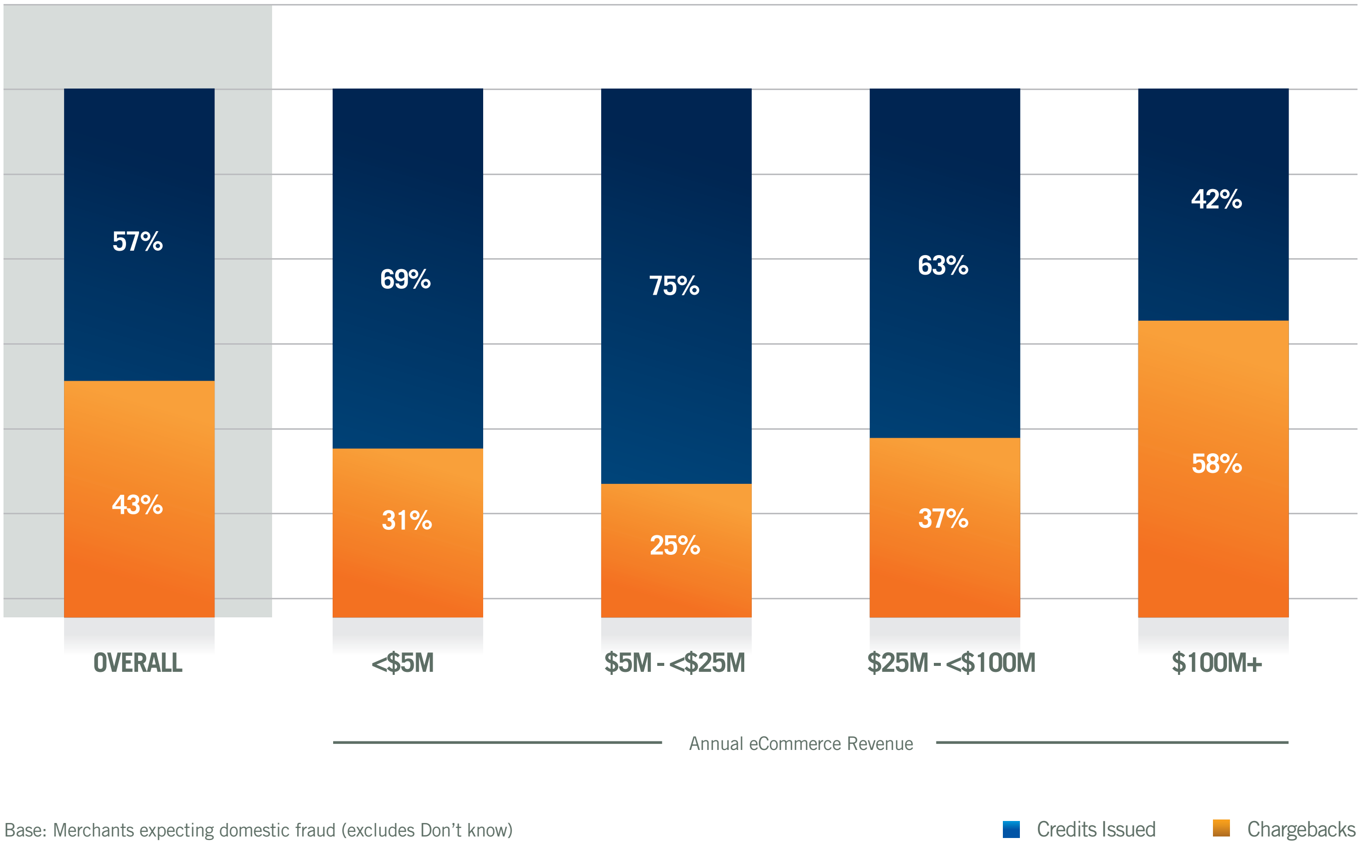
🟩 Fraud Rate - by Order, Domestic* 🟦 Fraud Rate - by Order, International**

© 2013 CyberSource Corporation, a Visa company. All rights reserved.

Although chargebacks are the most often cited metric, companies report that chargebacks account for only 43% of all fraud claims.

% OF FRAUD CLAIMS: CHARGEBACKS VS. CREDITS ISSUED BY MERCHANT

(OVERALL AND BY MERCHANT SIZE)

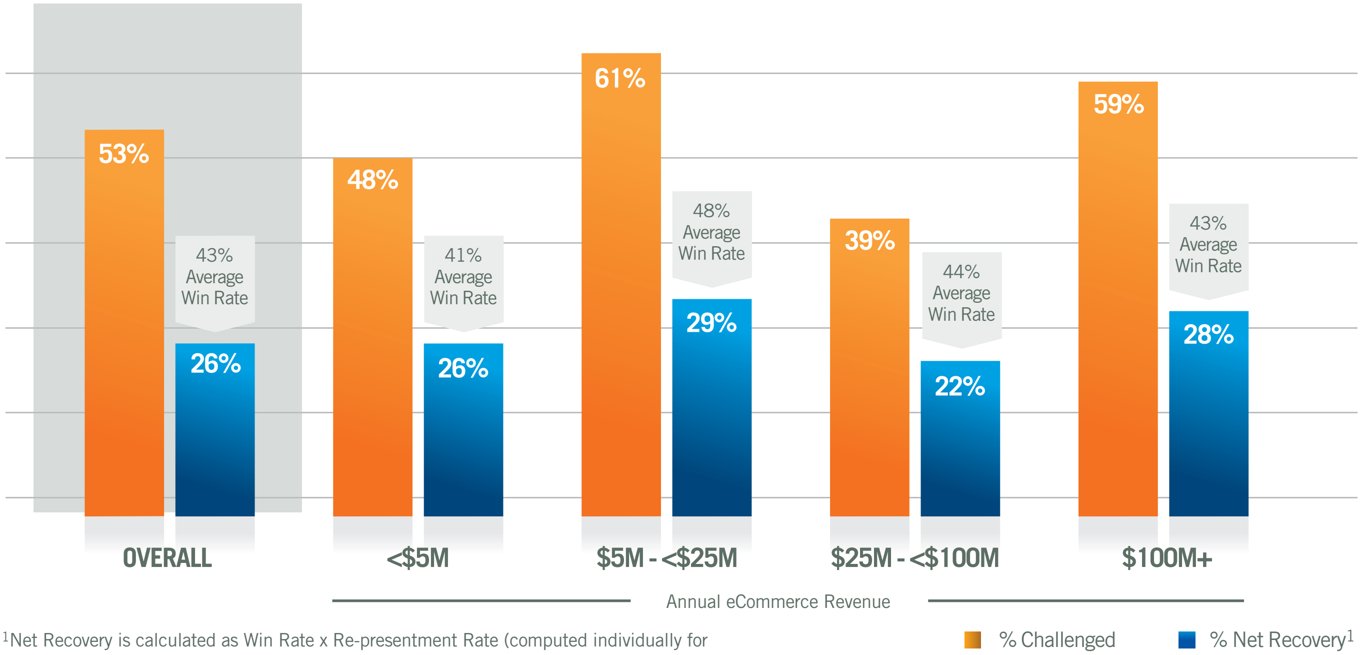


Base: Merchants expecting domestic fraud (excludes Don't know)

© 2013 CyberSource Corporation, a Visa company. All rights reserved.

FRAUD CHARGEBACK RE-PRESENTMENT: WIN RATE/NET RECOVERY RATE

(OVERALL AND BY MERCHANT SIZE)



[1]Net Recovery is calculated as Win Rate x Re-presentment Rate (computed individually for respondents who answered both questions, then averaged)

UPDATES TO VISA INC.'S CHARGEBACK AND DISPUTE RESOLUTION PROCESS[5]

In April 2013, Visa will institute changes in chargeback rules to streamline the dispute resolution process overall (effective globally, excluding Visa Europe). Below is a quick review of what's ahead (effective on or after April 20, 2013):

1. **Compelling Evidence Reason Codes.** Merchants will have additional representment rights to provide compelling evidence for chargeback Reason Codes 30 (Services Not Provided or Merchandise Not Received), 53 (Not as Described or Defective Merchandise), 81 (Fraud – Card-Present Environment), and 83 (Fraud – Card-Absent Environment). These are only new representment rights to provide compelling evidence and not a remedy for the chargeback.

2. **Issuers Must Address Compelling Evidence.** If compelling evidence is provided by the acquirer with the representment, issuers must attempt to contact their cardholder with this new information.

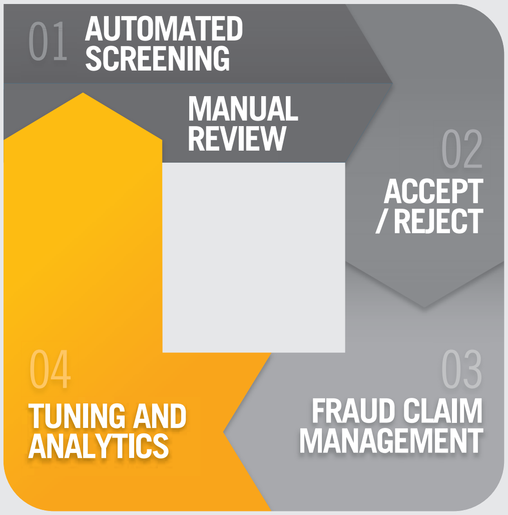
3. **Pre-Arbitration Requirement for Issuers.** If the issuer refutes the compelling evidence provided with the representment by the acquirer, the issuer must initiate a pre-arbitration case prior to filing arbitration with Visa.

A table outlining Allowable Compelling Evidence by Reason Code is available for reference (see footnoted URL). For more information on these changes, please contact your acquiring bank, processor or Visa representative.

[5] http://usa.visa.com/download/merchants/compelling-evidence-dispute-resolution.pdf

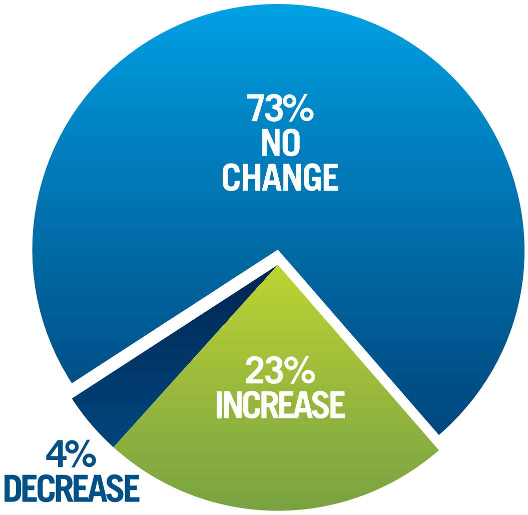
© 2013 CyberSource Corporation, a Visa company. All rights reserved.

TUNING AND ANALYTICS



For most companies, budgets and resources remain unchanged in 2013. Similar to last year, the order review staff comprises over half of an organization's budget for fraud management.

EXPECTED BUDGET CHANGE FOR FRAUD MANAGEMENT 2013



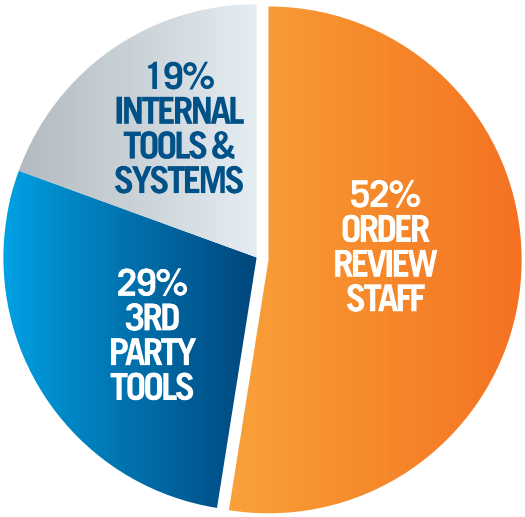
AVERAGE* % FRAUD MANAGEMENT BUDGET EXPECTED TO DECREASE
25%

AVERAGE* % FRAUD MANAGEMENT BUDGET EXPECTED TO INCREASE
10%

*Median used

© 2013 CyberSource Corporation, a Visa company. All rights reserved.

AVERAGE % SPENDING ALLOCATION FOR FRAUD MANAGEMENT 2013



PLANNED STAFFING LEVELS FOR FUTURE

23%	69%	8%
Increase	Same	Decrease

Base: Merchants who manually review to screen for eCommerce fraud (Excluding Don't know / No answer)

Base: Total Merchants (excludes No answer)

PERCEIVED FRAUD THREATS

In 2012, the Merchant Risk Council (MRC) partnered with CyberSource to survey its members on the top fraud attacks[6] that were most impactful to them, by frequency of attack and revenue loss. In ranked order, the top nine fraud attacks were:

1. Clean Fraud
2. Account Takeover
3. Friendly Fraud
4. Identity Theft
5. Affiliate Fraud
6. Re-shipping
7. Botnets
8. Phishing/Pharming/Whaling
9. Triangulation Schemes

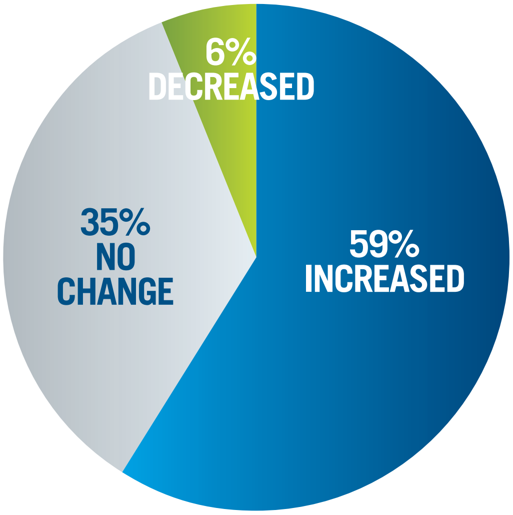
Respondents to this year's CyberSource Online Fraud Survey shed some light into the top three. Nearly 60% say that friendly fraud[7] has increased over the last two years, and over half say that the impact of account takeover is significant on their business. Yet on the positive side, nearly 2/3 say that fraud detection is either the same or easier in comparison to 12 months ago.

[6] To listen to a recorded webinar of this research, go to www.cybersource.com/top9fraudtrends

[7] Defined as the actual cardholder or someone known to the cardholder (such as a family member) making a legitimate purchase and then subsequently disputing the charge (charging back), claiming never to have purchased or received the goods.

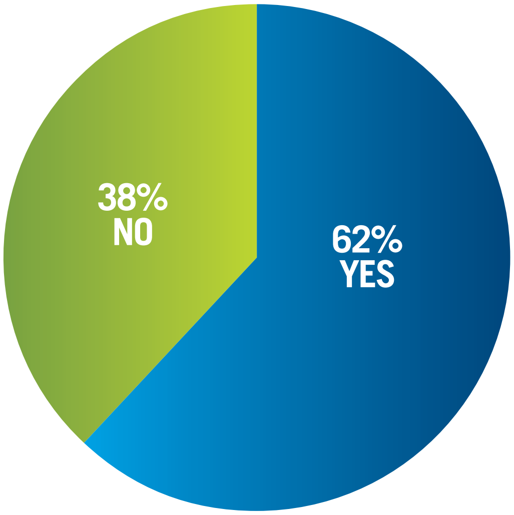
© 2013 CyberSource Corporation, a Visa company. All rights reserved.

PERCEPTION OF FRIENDLY FRAUD OVER THE LAST 2 YEARS



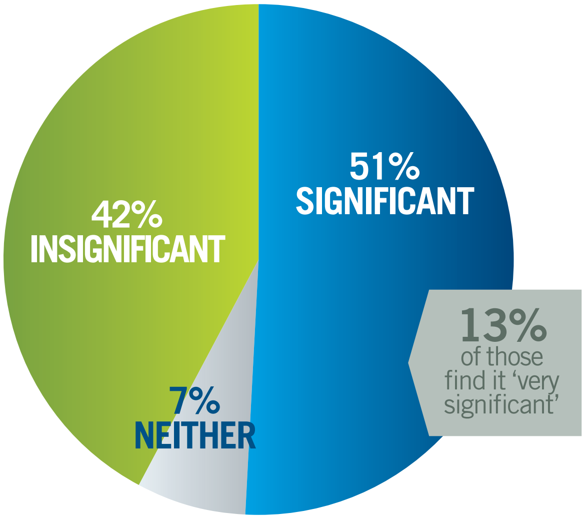
Base: Merchants with annual eCommerce revenue $25M+ (excludes Don't know)

SAME TOOLS USED FOR ACCOUNT TAKEOVER AND ORDER SCREENING



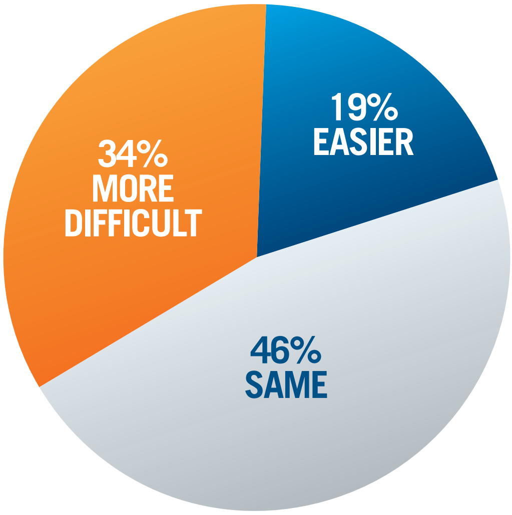
Base: Merchants with annual eCommerce revenue $25M+ (excludes Don't know / No answer)

SIGNIFICANCE OF ACCOUNT TAKEOVER ON BUSINESS



Base: Merchants with annual eCommerce revenue $25M+ (excludes Don't know / those without registered account users)

EASE OF FRAUD DETECTION COMPARED TO 12 MONTHS AGO



Base: Total Merchants (excludes Don't know)

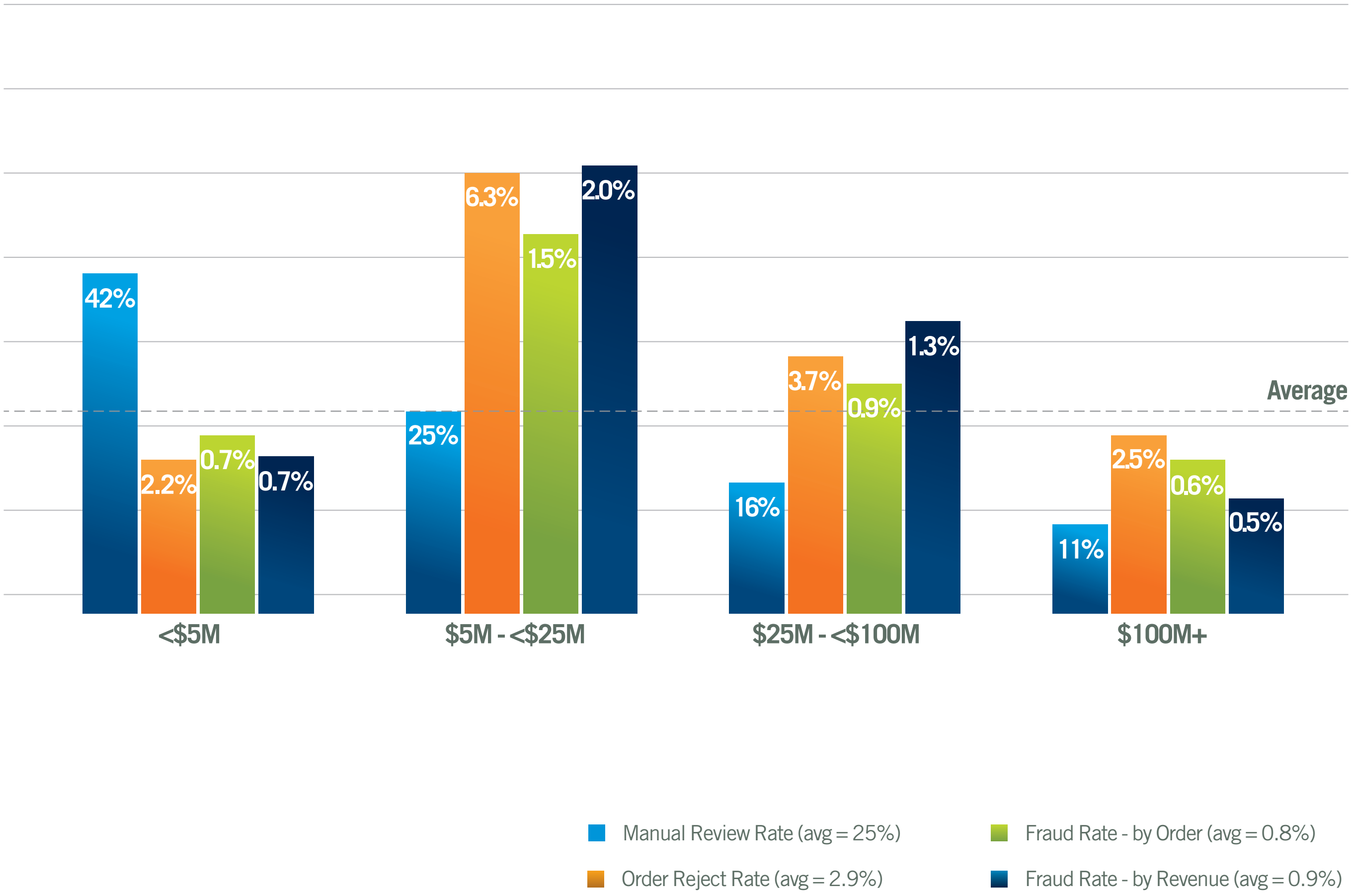
© 2013 CyberSource Corporation, a Visa company. All rights reserved.

CONCLUSION

To provide an overall assessment and basis for comparison, we took a snapshot of average survey respondent performance across four key performance indicators (KPIs): manual review rate, order rejection rate, fraud rate by order, and fraud rate by revenue, highlighting KPIs by industry and organizational size. KPIs will vary, as each company is unique in terms of their business objectives, resources, expertise, fraud tolerance and risk.

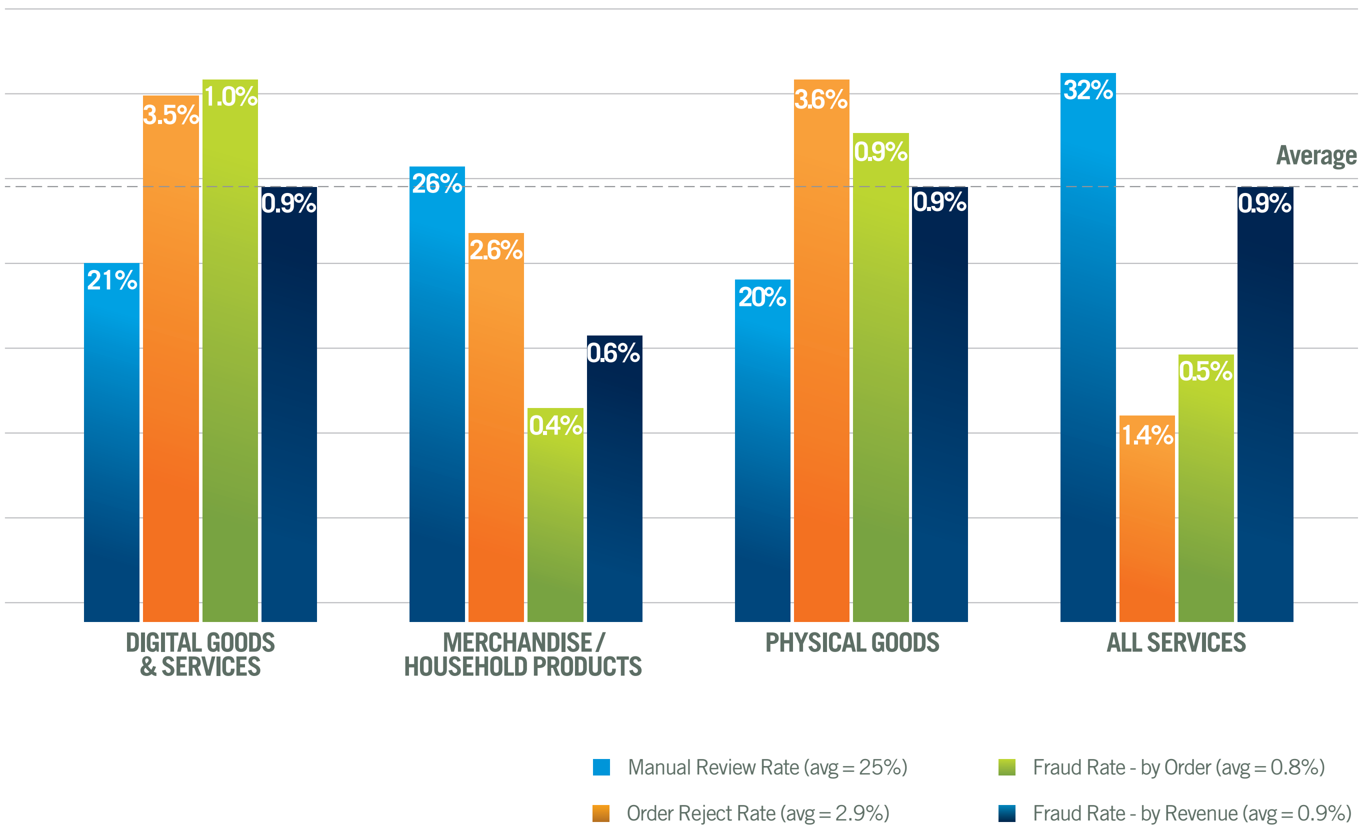
Companies constantly weigh the tradeoffs among fraud loss, customer experience, and cost, in tuning their operations to protect against the latest fraud attacks. Though it is unlikely that fraud can ever be eliminated completely, organizations can effectively manage fraud with the right systems, people, and processes in place.

KPIs BY MERCHANT SIZE



© 2013 CyberSource Corporation, a Visa company. All rights reserved.

KPIs BY SELECT INDUSTRIES



© 2013 CyberSource Corporation, a Visa company. All rights reserved.

RESOURCES & SOLUTIONS

To find information on CyberSource's industry-leading fraud management solutions, self-paced webinars, and other whitepapers on payment management, visit www.cybersource.com.

CYBERSOURCE FRAUD MANAGEMENT SOLUTIONS

CyberSource, an industry leader in fraud management solutions, enables businesses to continually improve profitability by detecting fraud sooner and more accurately and by streamlining fraud management operations. CyberSource provides a complete range of solutions, including training, consultation, active management of fraud screening, and outsourcing all or part of your fraud management operations.

Decision Manager, our hosted fraud management system, serves as the foundation for CyberSource Fraud Management Solutions. Featuring the world's largest fraud detection radar, Decision Manager provides access to a full range of data generated from global fraud detectors, multi-merchant and cross-industry correlations, truth data and more, across sales channels and geographies. It features a highly flexible rules engine backed by powerful statistical risk models, a customizable case management system, and detailed reporting and analytics.

Our fraud solutions are led by analysts with 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 ensure your fraud losses are minimized while keeping your operations running efficiently. In addition, CyberSource has a multi-lingual review team of experts providing your business with 24/7 risk screening capability. All of our fraud experts maintain rigorous ongoing training and performance monitoring to ensure consistently high quality results are achieved.

Chargeback Management Service– ENHANCED!
CyberSource chargeback experts perform detailed analysis of your chargebacks and provide best practice advice for your fraud operations to prevent future chargebacks. We manage the entire chargeback recovery process – receipt and review, interaction with banks, and re-presentment documentation--to ensure that you maximize profitability with the least impact to your operations.

REPORT & SURVEY METHODOLOGY

This survey was conducted via online questionnaire by Mindwave Research. Participating organizations completed the survey September 12 – October 12, 2012. All participants were either responsible for or influenced decisions regarding risk management in their companies. 13% of the survey participants use CyberSource fraud management solutions.

This report is based on a survey of U.S. and Canadian online merchants. Decision makers who participated in this survey represent a blend of small, medium and large-sized organizations based in North America. Experience levels range from companies in their first year of online transactions to some of the largest retailers and digital distribution entities in the world. Companies participating in the survey reported a total estimate of more than $105 billion for their 2012 online sales.

SUMMARY OF PARTICIPANT PROFILES

Online Fraud Survey Wave	2008	2009	2010	2011	2012
Total number of companies participating	400	352	334	325	312
Annual Online Revenue					
Less than $5M	53%	55%	54%	56%	46%
$5M to less than $25M	18%	14%	14%	15%	16%
$25M or more	29%	31%	32%	29%	38%
Duration of Online Selling					
Less than 1 year	11%	5%	6%	5%	4%
1 – 2 years	12%	16%	11%	12%	7%
3 – 4 years	13%	14%	19%	15%	18%
5 or more years	64%	65%	64%	68%	71%
Risk Responsibility					
Ultimately responsible	58%	54%	55%	50%	47%
Influence decision	42%	46%	45%	50%	53%

© 2013 CyberSource Corporation, a Visa company. All rights reserved.

About CyberSource

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, and maintains offices throughout the world, with regional headquarters in Singapore, Tokyo, Miami, Sao Paulo and Reading, U.K. CyberSource operates in Europe under agreement with Visa Europe. For more information, please visit www.cybersource.com.

North America
CyberSource HQ
Phone: +1 888 330 2300
+1 650 432 7350
Email: sales@cybersource.com

Latin America and the Caribbean (LAC)
CyberSource Ltda.
Phone: +1 305 328 1998
Email: lac@cybersource.com

Europe
CyberSource Ltd.
Phone: +44 (0) 118 990 7300
Email: uk@cybersource.com

Asia Pacific
CYBS Singapore Pte Ltd.
Email: ap_enquiries@cybersource.com

Japan
CyberSource KK
Phone: +81 (0) 3 3548 9873
Email: sales@cybersource.co.jp