Report & Survey Methodology

The survey was conducted via online questionnaire by Mindwave Research. Participating organizations completed the survey between September 13th and October 12th 2011. All participants were either responsible for or influenced decisions regarding risk management in their companies. 12% 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. Merchant 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. Merchants participating in the survey reported a total estimate of more than $83 billion for their 2011 online sales.

<table>
<thead>
<tr>
<th>Summary of Participants’ Profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online Fraud Survey Wave</td>
</tr>
<tr>
<td>Total number of merchants</td>
</tr>
<tr>
<td>participating</td>
</tr>
<tr>
<td>2007  2008  2009  2010  2011</td>
</tr>
<tr>
<td>318  400  352  334  325</td>
</tr>
<tr>
<td>Annual Online Revenue</td>
</tr>
<tr>
<td>Less than $5M</td>
</tr>
<tr>
<td>2007  2008  2009  2010  2011</td>
</tr>
<tr>
<td>56%  53%  55%  54%  56%</td>
</tr>
<tr>
<td>$5M to Less than $25M</td>
</tr>
<tr>
<td>2007  2008  2009  2010  2011</td>
</tr>
<tr>
<td>15%  18%  14%  14%  15%</td>
</tr>
<tr>
<td>$25M or More</td>
</tr>
<tr>
<td>2007  2008  2009  2010  2011</td>
</tr>
<tr>
<td>29%  30%  31%  32%  29%</td>
</tr>
<tr>
<td>Duration of Online Selling</td>
</tr>
<tr>
<td>Less than One Year</td>
</tr>
<tr>
<td>2007  2008  2009  2010  2011</td>
</tr>
<tr>
<td>5%  11%  5%  6%  5%</td>
</tr>
<tr>
<td>1-2 Years</td>
</tr>
<tr>
<td>2007  2008  2009  2010  2011</td>
</tr>
<tr>
<td>13%  12%  16%  11%  12%</td>
</tr>
<tr>
<td>3-4 Years</td>
</tr>
<tr>
<td>2007  2008  2009  2010  2011</td>
</tr>
<tr>
<td>16%  13%  14%  19%  15%</td>
</tr>
<tr>
<td>5 or More Years</td>
</tr>
<tr>
<td>2007  2008  2009  2010  2011</td>
</tr>
<tr>
<td>66%  64%  65%  64%  68%</td>
</tr>
<tr>
<td>Risk Management Responsibility</td>
</tr>
<tr>
<td>Ultimately Responsible</td>
</tr>
<tr>
<td>2007  2008  2009  2010  2011</td>
</tr>
<tr>
<td>55%  58%  54%  55%  50%</td>
</tr>
<tr>
<td>Influence Decision</td>
</tr>
<tr>
<td>2007  2008  2009  2010  2011</td>
</tr>
<tr>
<td>45%  42%  46%  45%  50%</td>
</tr>
</tbody>
</table>

Get Tailored Views of Risk Management Pipeline™ Metrics

For sales assistance or to get a view crafted for your company’s size and industry, please contact CyberSource at +1 888 330 2300 (international: +1 650 432 7350) or online at www.cybersource.com/contact_us.

For additional information, whitepapers and webinars:

- **Fraud Management Solutions:** visit www.cybersource.com/products_and_services/fraud_management/
- **Global Payment Solutions:** visit www.cybersource.com/products_and_services/global_payment_services/
- **Payment Security Solutions:** visit www.cybersource.com/products_and_services/payment_security/
# Table of Contents

**EXECUTIVE SUMMARY** ........................................................................................................ 1

**STAGE 1: AUTOMATED SCREENING** ........................................................................... 3
  - Fraud Detection Tools Used During Automated Screening ............................................ 3
  - Planned Automated Screening Tool Usage 2012 ........................................................... 4
  - Automated Decision/Rules Systems .............................................................................. 4

**STAGE 2: MANUAL REVIEW** ...................................................................................... 6
  - Manual Order Review Rates ......................................................................................... 6
  - Tools Used/Planned During Manual Review .................................................................... 7
  - Review Operations Efficiency ....................................................................................... 7

**STAGE 3: ORDER DISPOSITIONING (ACCEPT/REJECT)** .......................................... 9
  - Post-Review Order Acceptance Rates ............................................................................. 9
  - Overall Order Rejection Rates ....................................................................................... 9
  - International Orders Riskier .......................................................................................... 10
  - Estimating Valid Order Rejection .................................................................................. 10

**STAGE 4: FRAUD CLAIM MANAGEMENT** ............................................................... 11
  - Types of Fraudulent Transactions ............................................................................... 11
  - Friendly Fraud ............................................................................................................. 11
  - Fighting Chargebacks ................................................................................................ 11
  - Fraud Rate Metrics ...................................................................................................... 12

**TUNING & MANAGEMENT** ..................................................................................... 14
  - Clean Fraud Still a Problem .......................................................................................... 14
  - Tracking Mobile Fraud ................................................................................................ 14
  - Size of Fraud Management Budgets .............................................................................. 14
  - Budget Allocation ........................................................................................................ 15

**CONCLUSION** ........................................................................................................ 16

**RESOURCES & SOLUTIONS** ................................................................................... 17

**ABOUT CYBERSOURCE** .......................................................................................... 18
Executive Summary

Managing online fraud continues to be a significant and growing cost for merchants of all sizes. To better understand the impact of payment fraud for online merchants, CyberSource sponsors annual surveys addressing the detection, prevention and management of online fraud. This report summarizes findings from our 13th annual survey. Note: this report provides benchmarks on total fraud rates (chargebacks and credits issued directly to consumers by merchants). 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.

Estimated $3.4 Billion Lost to Online Fraud

In 2011, merchants reported losing an average of 1.0% of total online revenue to fraud. Although 2011 showed an uptick in revenue loss rate versus the prior year, merchants reported a 33% decrease in the percent of orders lost to fraud, 0.6%. Using 2011 industry market projections1 on eCommerce in North America, we estimate that the total revenue loss translates to approximately $3.4 billion, a $700 million increase over 2010 results (see Chart #1).

In 2011, the order rejection rate continued to increase as it has done since 2009. Merchants reported that they reject an average of 2.8% of orders due to suspicion of payment fraud.

Chargebacks Account for less than 50% of Fraud

This year’s survey probed the percent of fraud losses accounted for by chargebacks. Overall, merchants continue to report that chargebacks accounted for less than half of fraud losses — 41%, on average. The majority of fraud loss is due to merchants issuing a credit to reverse a charge in response to a consumer’s claim of fraudulent account use, or because of subsequent information from additional orders that indicate likelihood of fraud on the recently placed order. For digital goods with instant fulfillment, credits could be issued afterwards, once fraud has been detected.

International Order Acceptance is Riskier

Accepting international orders is riskier than domestic orders. Merchants reported an international fraud rate by order rate of 2.0%, more than three times higher than domestic. In response to the higher perceived risk, merchants rejected international orders at a rate nearly three times higher than domestic (7.3% vs. 2.8%, respectively).

Note: this report provides benchmarks on total fraud rates (chargebacks and credits issued directly to consumers by merchants). 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 an 8% uplift to account for the merchant segments covered by the survey but not by eMarketer’s market sizing.
Manual Review Rates are Slightly Up
After remaining at 72% in the last two years, the percent of merchants conducting manual review increased to 75% in 2011, with 27% of orders routed to manual review (vs. 24% in 2010). Merchants continue to rely heavily on manual review teams as a defense against fraud, with the review teams accessing an average of 4.2 systems to research and disposition the order (vs. 4.0 in 2010).

Opportunities to Streamline Fraud Management
As eCommerce sales continue to grow, scalability will become more of a pressing issue. Merchants continue to face the challenge of screening more online orders while keeping manual review staffing and fraud rates as low as possible. Yet 82% of merchants reported that their fraud budgets will stay the same or decrease, and only 18% reported that they will be increasing their order review staff.

With more volume and limited resources, emphasizing and improving automated fraud detection capabilities is a top priority for 55% of the merchants surveyed. The need for better automation is understandable when 75% of manually reviewed orders are ultimately accepted. To be successful, fraud managers will need to adopt tools and practices to reduce the number of orders being routed to review, as well as enable their review teams to operate more efficiently.

Mobile Fraud Risk is Mostly Unknown
This year, we asked about merchant perception of fraud in the mobile channel, which we defined as either commerce on a mobile-optimized website or through a mobile app. Overall, 92% of merchants do not know their mobile fraud rates, 7% perceive that mobile fraud rates are the same or lower than online fraud, while 1% perceive mobile fraud to be slightly higher.

Total Risk Management Pipeline View
Businesses that concentrate solely on minimizing chargebacks may not see the complete financial picture. Online payment fraud impacts profits from online sales in multiple ways. Besides direct revenue losses, the cost of stolen goods/services and associated delivery/fulfillment costs, there are the additional customer experience “costs” of rejecting valid orders, staffing manual review, administration of fraud claims, as well as challenges with scaling fraud management operations as business grows. Merchants can realize certain efficiencies by taking a total risk management pipeline view of operations and costs. While the fraud rate is one metric to monitor (and maintain within industry and card scheme limits), an end-to-end view is required to achieve the optimal financial outcome.

In 2011, these “profit leaks” in the Risk Management Pipeline™ impact as much as 30% of orders for mid-sized merchants and as much as 13% of orders for larger merchants—driven primarily by too many orders being manually reviewed, which restricts profits, operating efficiency and scalability. This report details key metrics and practices at each point in the pipeline to provide you with benchmarks and insight. Custom views of these benchmarks and practices are available through CyberSource—see end of report for contact information.
### Fraud Detection Tools Used During Automated Screening

We define fraud detection tools as those used to assess the probability of risk associated with a transaction. They are categorized into four groups: validation services, proprietary data, purchase device tracing, and multi-merchant data. Results from these tools drive the decision to accept, reject or review the transaction, either through an automated rules-based system or manually. In 2011, 56% of merchants surveyed utilize an automated screening system.

Of these, 68% of merchants report using at least 3 tools in their automated screening solution and an average of 4.9 tools overall. Larger merchants processing higher order volumes use an average of 8 tools. Sheer order volume could necessitate automated screening or more sophistication to address fraud, as well drive fraudsters to target these merchants more often. In addition, larger merchants consistently show higher utilization of more tools, as shown in Chart #2, which highlights the most popular fraud detection tools used.

Ninety-seven percent of merchants use one or more validation tools. Some are provided by the card schemes, such as Card Verification Number (CVN), Address Verification Service (AVS), and payer authentication services (Verified by Visa, MasterCard SecureCode), and others are provided by third-party verification services.

Not surprisingly, CVN and AVS show the most widespread adoption, as they are provided at no additional cost. But in terms of effectiveness, with the larger merchants, few cited CVN and AVS in one of their top three tools in terms of effectiveness (see Chart #3). This could be explained by the relative ease of obtaining CVNs on the black market, and the limited availability of AVS data outside of North America.

In terms of leveraging customer history, 67% of merchants currently use or are planning to use their own proprietary data. In particular, the use of company-specific fraud-scoring models and customer website behavior analysis grew in 2011.

### Stage 1: Automated Screening

<table>
<thead>
<tr>
<th>Order Retained</th>
<th>Automated Screening</th>
<th>Manual Review</th>
<th>Accept / Reject</th>
<th>Fraud Claim Management</th>
<th>Retained Revenue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tuning and Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Fraud Detection Tool Usage 2011

#### All Merchants

<table>
<thead>
<tr>
<th>Validation Services (Net)</th>
<th>Address Verification Service (AVS)</th>
<th>Postal address validation services</th>
<th>Verified by Visa/MasterCard SecureCode</th>
<th>Telephone # verification/reverse lookup</th>
<th>Social networking sites</th>
<th>Paid-for public records services</th>
<th>Credit history check</th>
<th>Out-of-wallet or in-wallet challenge/response systems</th>
<th>Customer order history</th>
<th>Negative lists (in-house lists)</th>
<th>Order velocity monitoring</th>
<th>Fraud scoring model – company specific</th>
<th>Customer website behavior analysis</th>
<th>Positive lists</th>
<th>IP geolocation information</th>
<th>Device “fingerprinting”</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>97</td>
<td>79</td>
<td>38</td>
<td>25</td>
<td>22</td>
<td>10</td>
<td>3</td>
<td>1</td>
<td>7</td>
<td>45</td>
<td>14</td>
<td>8</td>
<td>6</td>
<td>10</td>
<td>1</td>
<td>10</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

#### Merchants $25M+ Online Revenue

<table>
<thead>
<tr>
<th>Validation Services (Net)</th>
<th>Address Verification Service (AVS)</th>
<th>Postal address validation services</th>
<th>Verified by Visa/MasterCard SecureCode</th>
<th>Telephone # verification/reverse lookup</th>
<th>Social networking sites</th>
<th>Paid-for public records services</th>
<th>Credit history check</th>
<th>Out-of-wallet or in-wallet challenge/response systems</th>
<th>Customer order history</th>
<th>Negative lists (in-house lists)</th>
<th>Order velocity monitoring</th>
<th>Fraud scoring model – company specific</th>
<th>Customer website behavior analysis</th>
<th>Positive lists</th>
<th>IP geolocation information</th>
<th>Device “fingerprinting”</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>86</td>
<td>47</td>
<td>24</td>
<td>29</td>
<td>20</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>69</td>
<td>1</td>
<td>6</td>
<td>5</td>
<td>10</td>
<td>1</td>
<td>10</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

© CyberSource Corporation. All rights reserved.
Customer website behavior analysis is one of the newer fraud tools available. It attempts to assess whether or not the customer’s visit and website activity is consistent with that of a typical user. For instance, the time spent on checkout or the number of pages viewed varies greatly between a typical user and a fraudster using a bot. Although adoption is currently relatively low, it may increase as fraudsters learn how to circumvent traditional mitigation tools.

Purchase device tracing are tools that attempt to validate the device and location of the network from which the order is being placed. They continue to show broader adoption. For the fraudster, bypassing device fingerprinting and IP geolocation requires more sophistication than just obtaining stolen customer identity and payment data. As a result, device fingerprinting and IP geolocation were cited most often by large merchants as one of their top three effective tools.

Multi-merchant data and purchase history is less utilized in comparison to the other three categories, but can be quite useful to merchants. Statistically, the average top ten Internet merchant sees only 1/100th of the actual annual online transaction activity, at best. Multi-merchant data gives a wider view of activity to detect subtle fraud patterns, by providing a broader pool of transactions for merchants to analyze for linkages and potential fraud.

Multi-merchant data can be difficult to obtain without the use of a third-party provider, due to legal and privacy regulations. Similarly, shared negative lists are subject to legal regulations and are only as good as the information provided by others — and in some cases the data can be outdated or inaccurate. Shared data is only effective if there is a sufficiently large volume of current, accurate data to correlate and analyze. The use of shared negative lists fell by 3% among large merchants, yet use of multi-merchant purchase velocity increased by 16% (vs. 2010). For merchants of all sizes, shared negative lists grew by 2%, and multi-merchant purchase velocity grew by 6%.

### Planned Automated Screening Tool Usage 2012

**Device Fingerprinting Highest on “Plan to Buy” Lists**
Fifty-seven percent of surveyed merchants plan to add one or more new fraud detection tools in the next twelve months. Device fingerprinting and customer website behavior analytics are the two tools that most merchants expect to evaluate for adoption in the next year.

As in past years, card scheme payer authentication services figure prominently in merchants’ future plans. The 2011 survey results show that 25% of merchants currently use one or more of the available payer authentication services, and 20% say they are interested in deploying within the next twelve months.

Despite significant interest in implementing payer authentication systems over the past few years, we have seen relatively slow adoption of payer authentication since we started tracking this tool in 2003. But with recent bank and regulatory mandates on using payer authentication, particularly abroad, merchant adoption is expected to increase, at least for those merchants that have localized websites.

### Automated Decision/Rules Systems

#### Automated Order Screening
Fifty-six percent of merchants utilize an automated decisioning system. These systems apply a merchant’s business rules to...
evaluate risk on incoming orders in real-time. As companies grow in size and the number of fraud detection tools increases, leveraging these assets as part of an automated order screening solution will become increasingly imperative. Decision systems can help organizations quickly analyze data from incoming transactions and assess their risk, thereby enabling merchants to scale their businesses as order volumes increase.

Because fraud patterns are dynamic, automated screening systems allow merchants to implement changes quickly; 54% of merchants say that changes are implemented instantly. Furthermore, over 80% of the merchants surveyed have a confidence level of 75% or higher that the changes implemented will have the intended results.

**Results of Automated Screening**

The automated order screening process generates three outcomes: 1) order acceptance without further review, 2) orders flagged for further review and 3) automatic order rejection. Some merchants allow this initial automated screen to cancel orders without further human intervention. Forty-eight percent of all merchants cancelled some orders as a result of their automated screening process and 60% of large merchants indicated they cancelled some orders at this stage (see Chart #4).

### Are Inbound Orders Rejected Based Solely On Automated Screening?

- **All Merchants**
  - Yes: 48%
  - No: 52%
  - 13%

- **Merchants $25M+ Online Revenue**
  - Yes: 60%
  - No: 40%
  - 17%

**Yes**, but generally ONLY if customer is on our negative list

**Yes**, if automated tests indicate too much risk OR customer is on our negative list

**No**, generally all suspicious orders are outsourced for manual review

![Chart #4](image-url)
Orders which do not pass the automated order screening stage typically enter a manual review queue. During manual review, additional information is often collected to determine if orders should be accepted or rejected due to excessive fraud risk.

Manual review is often the largest portion of an organization’s fraud management operations, representing just over half of the budget. Staff overhead is costly, limits scalability and could potentially impact customer satisfaction as order volume increases, due to the inherent latency associated with manual review processes.

Seventy-five percent of merchants surveyed do not anticipate a change in staffing levels in 2012, yet retail eCommerce is forecasted to grow by 11.3% in 2012. This presents significant challenges to profit growth, especially if the total number of orders to be manually reviewed increases in lockstep with the total increase of online sales.

Merchants could divert more staff time to order review, or increase staffing levels, but both options would increase overhead costs. Alternatively, merchants can allow more time to process orders, but they would need to consider impacts to customer service in the event of shipping delays. Another option would be to fine-tune their automated decisioning system to accurately disposition more orders up front, thereby sending fewer orders to manual review.

**Manual Order Review Rates**

Seventy-five percent of merchants surveyed conduct manual review, a percentage that has remained relatively stable over the last few years. For those merchants that do conduct manual reviews, the percentage of all orders that are manually reviewed increased slightly, to 27% (see Chart #5). Review rates for merchants with up to $25 million in online sales are more than double those of larger merchants (see Chart #6). Lower order volume and the lack of an automated order screening system may account for the higher review rates — only 43% of these smaller merchants have an automated order screening system.

---

2 eMarketer, “U.S. Retail Sales, 2009 - 2015”
Tools Used/Planned During Manual Review

Although many of the same fraud detection tools are used for both automated and manual reviews, the review team typically leverages additional tools and processes when attempting to validate an order. “Customer order history” and “Contacting the customer” continue to be employed most often. The tools that have seen the highest growth in adoption are Google Maps for investigating delivery addresses, along with IP geolocation (see Chart #7).

In addition to the aforementioned tools, “Using device fingerprinting results” (where results of device fingerprinting information are exposed in the manual review screens) and “Postal address validation services” have seen more adoption with large merchants in 2011. “Using device fingerprinting results” was the most cited by merchants as a technology they would most likely be implementing in 2012.

Review Operations Efficiency

Reviewer Efficiency

The median number of orders a reviewer processes in a day ranged from 6 for small merchants to 100 for large merchants (see Chart #8). Large merchants who have case management systems typically achieve twice the throughput per reviewer in the manual review stage, in part due to more sophisticated review systems and experienced investigators.

Orders Manually Reviewed per Day, Per Reviewer

<table>
<thead>
<tr>
<th></th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall</td>
<td>60</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>&lt;$5M</td>
<td>5</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>&lt;$25M</td>
<td>60</td>
<td>50</td>
<td>45</td>
</tr>
<tr>
<td>&lt;$100M</td>
<td>150</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>&lt;$100M</td>
<td>100</td>
<td>100</td>
<td>100</td>
</tr>
</tbody>
</table>

Merchants reported that reviewers accessed or input data into an average of 4.2 systems, with 10% of merchants reporting usage of 10 or more systems. The inability to seamlessly integrate or automatically interface with these multiple systems negatively impacts reviewer productivity, which is exacerbated as the number of systems in use increases.

Final Order Disposition

Automated screening and manual order review ultimately result in order acceptance or rejection. A relatively high percentage of orders manually reviewed are ultimately accepted (see next section). This highlights the need for merchants to continue improving automated screening accuracy and reduce their reliance on expensive manual review processes. A look at order reject and acceptance rates follows in Stage 3 of the pipeline review.
To optimize the manual review process, focus on how your reviewers can access the information they need in the most intuitive and direct way possible. Use a case management system that can consolidate all of the information relating to the order in one place.

Provide a structured framework and checklist for investigating orders to your review team, which help to streamline the process and ensure consistency in dispositioning orders.

Finally, measure the performance of your review team by looking at key metrics (such as orders reviewed per day, length of time in queue, chargebacks from the manual review process and by reviewer), to identify areas for improvement at both the reviewer and team level.
Stage 3: Order Dispositioning (Accept/Reject)

Post-Review Order Acceptance Rates
Of the orders that are manually reviewed, on average, 75% of them are ultimately accepted. Over half of the merchants surveyed state that they accept over 90% of the orders placed into review (see Chart #9). With three out of every four orders accepted, these merchants are incurring significant expense to review legitimate orders (see Chart #10). Either excessively high acceptance or rejection rates can indicate more orders than necessary are being diverted to manual review, a situation that can be corrected by tuning automated screening rules/detectors to isolate and systematically disposition more of these orders.

Overall Order Rejection Rates
Order reject rates can either reflect true fraud risk or signal a potential “profit leak” in terms of customer insults. In 2011, merchants reported rejecting an average of 2.8% of orders domestically (see Chart #11).
Merchants with more than $100 million in online sales continued to make progress in reducing rejection rates, while smaller merchants with less than $5 million in online sales showed slightly higher rejection rates. As expected, merchants selling higher ticket, physical goods tend to reject more orders (i.e., consumer electronics, apparel/jewelry) in comparison to digital goods (see Chart #12).

International Orders Riskier

The order rejection rate for international orders is nearly three times higher than domestic orders — 7.3% vs. 2.8%, respectively (see Chart #13). Fraud screening is more challenging for international orders, as standard validation tools may not be readily available or may be more costly to implement. Address and telephone records, credit checks, and public records vary by country. The actual fraud rate experienced on international orders supports a cautious approach to order acceptance, as merchants report the fraud risk on international orders is significantly higher than that of domestic orders.

Estimating Valid Order Rejection

Orders are rejected due to suspicion of fraud, but within that pool, inevitably, are valid orders from customers that were erroneously rejected. In addition to the lost sales from these good customers, merchants try to avoid this type of “customer insult,” as lost customers and negative word of mouth can adversely impact future revenues.

Fifty-two percent of large merchants surveyed attempt to estimate valid order rejection rates, but it is difficult to measure accurately or with a degree of confidence. Of the merchants that provided input on how they track valid order rejections, most cited tracking customer complaints or customer feedback on the orders. However, any of these methods understates the true “false positive” rate.

To focus the review team’s efforts on truly questionable orders, maximize the number of automated decisions. To this end, analyze the profiles of orders that are accepted during manual review and determine if there are common characteristics from which you could build effective “auto-pass” screening rules.

As a general rule of thumb, half of the orders that are manually reviewed should be accepted. Order acceptance and rejection rates that skew above 50% signal opportunities to shift more of the manual order evaluations to automated screening.
Types of Fraudulent Transactions
We define fraudulent orders as either chargebacks or a credits issued to consumers claiming fraudulent use of their accounts. As a result, actual fraud rates reported tend to be higher than those cited by banks or card schemes. Fraudulent orders have a significant impact on bottom line profits. Although chargebacks are the most often cited metric, merchants report that chargebacks actually account for only 41% of all fraud claims (see Chart #14).

Friendly Fraud
“Friendly fraud” occurs when a merchant receives a claim because the cardholder denies making the purchase or receiving the order, yet the goods or services were actually received. In some instances, the order may have been placed by a family member or friend that has access to the buyer’s cardholder information. Chart #15 shows that 60% of merchants perceive friendly fraud has increased over the past two years.

Fighting Chargebacks
Merchant practices vary with respect to contesting chargebacks (“re-presentment”). On average, merchants re-present 56% of their fraud-coded chargebacks, with nearly 30% re-presenting all of their chargebacks (see Chart #16).

Considering the financial impact of both fraud claim routes (chargebacks and credit issuance/reversal), some merchants encourage direct consumer contact to address fraud claims and thus avoid chargebacks from the acquiring bank/processor.
CyberSource Online Fraud Report

MERCHANTS REPORT THAT THEY WIN, ON AVERAGE, 40% OF THE CHARGEBACKS THEY DISPUTE, RESULTING IN A NET RECOVERY RATE OF 27%. USING THE AVERAGE PERCENT OF CHARGEBACKS THAT ARE DISPUTED (56%), MULTIPLIED BY THE AVERAGE WIN RATE OF 40%, RESULTS IN A NET RECOVERY RATE OF 22% (MEANING 22% OF ALL FRAUD-CODED CHARGEBACKS ARE RECOVERED). HOWEVER, GIVEN THE WIDE DISPARITY IN THE CHARGEBACK RE-PRESENTMENT RATE, WHEN THESE ARE CALCULATED ON A MERCHANT-BY-MERCHANT BASIS AND THEN AVERAGED, THE RE-PRESENTMENT WIN RATE RISES TO 27% (SEE CHART #17).

FRAGMENT RATE METRICS

WHEN MONITORING THE LEVEL AND TREND OF ONLINE FRAUD LOSS, WE FOCUS ON THREE KEY METRICS: 1) FRAUD RATE BY REVENUE (REVENUE LOST TO FRAUD AS A PERCENT OF TOTAL ONLINE SALES); 2) FRAUD RATE BY ORDER (PERCENT OF ACCEPTED ORDERS WHICH TURN OUT TO BE FRAUDULENT); AND 3) THE AVERAGE VALUE OF A FRAUDULENT ORDER RELATIVE TO A VALID ORDER. FRAUD RATES VARY WIDELY BY MERCHANT AND DEPEND ON A VARIETY OF FACTORS, SUCH AS ONLINE SALES VOLUME, TYPE OF PRODUCTS OR SERVICES SOLD ONLINE, HOW SUCH PRODUCTS/SERVICES ARE DELIVERED AND PAID FOR, AND THE MERCHANT’S FRAUD PREVENTION CAPABILITIES. IT IS IMPORTANT THAT MERCHANTS TRACK KEY FRAUD METRICS OVER TIME AND EVALUATE THEIR PERFORMANCE RELATIVE TO THEIR PEER GROUP (BOTH SIZE AND INDUSTRY).

FRAGMENT RATE BY REVENUE

REVENUE LOSS MEASUREMENT INCLUDES NOT ONLY THE VALUE OF ORDERS ON WHICH FRAUDULENT CHARGEBACKS ARE RECEIVED, BUT ALSO THE COST OF ANY CREDITS ISSUED TO AVOID SUCH CHARGEBACKS. IN 2011, THE AVERAGE FRAUD RATE BY REVENUE WAS 1.0%. THE LARGEST MERCHANTS REPORTED SMALLER REVENUE LOSS RATES (0.4%) WHILE CONVERSELY, SMALLER MERCHANTS REPORTED UP TO THREE TIMES HIGHER (SEE CHART #18).

AVERAGE FRAUD RATE BY REVENUE 2011 VS. 2010

(OVERALL AND BY MERCHANT SIZE)
**Fraud Rate by Order**
Another key metric is the number of accepted orders that later turn out to be fraudulent, expressed as a percent of total accepted orders. In 2011, the fraud rate by order was 0.6%, and ranged from 0.4% to 1.2% (see Chart #19).

**Fraudulent Order Value**
Historically, fraudulent orders tend to have higher values than valid orders. In 2011, merchants reported a median fraudulent order value of $250, vs. $150 for the valid order value.

**International Orders Carry Higher Risk**
Fifty-eight percent of merchants surveyed accepted orders from outside the U.S. & Canada in 2011, with international sales accounting for 17% of total orders, on average. Because of the higher risk associated with cross-border transactions, one in four merchants surveyed stopped accepting orders from at least one country outside of North America. Fraud rates for international orders are more than three times higher than domestic orders (2.0% vs. 0.6%, respectively). However, the fraud rate for international orders has remained relatively stable since 2009 (see Chart #20).

To minimize overall chargebacks, take steps to reduce your exposure to friendly fraud. Clearly articulated terms and conditions that the customer must acknowledge at the outset often provide an effective front-line deterrent. Follow this with other safeguards, such as confirmation emails, activation links, or other online validations that require customer input or action.

For example, if your business is subscription-driven, send an email to the address provided, with a link to activate the account. This serves two purposes: first, if the email address is phony, then the fraudster will be unable to activate the account. Second, if the email account is valid, once the activation URL is clicked, you’ll have a trail that you can use in the event that the cardholder disputes charges.

Any or all of these safeguards will put you in a better position to deter fraud or re-present any subsequent chargeback, as you will have documentation of actions taken by the customer.

Balance the safeguards required against the customer experience — excessive customer friction would negatively impact your legitimate customers.

By configuring your order flow with the appropriate checks properly in place, you can maximize legitimate revenue while deterring friendly fraud.
Clean Fraud Still a Problem
We define “clean” fraud as fraudulent orders that look and behave like valid orders because they pass the typical fraud checks put in place by a merchant. Forty-six percent of merchants say that the fraudulent orders they’ve seen are “cleaner” than what they experienced a year ago (see Chart #21). This is down slightly from 2010 levels, but continues to be the biggest change that merchants have noticed in 2011.

Tracking Mobile Fraud
As the mobile channel continues to grow, merchants will need to understand how fraud impacts mobile commerce. One school of thought believes mobile is riskier (new channel, harder to identify the device or IP address), while another school of thought believes the opposite (closed mobile network, passcodes on phones, omnipresent device).

Twenty-seven percent of merchants reported that they have a mobile commerce website, while 20% reported having a mobile app (Note: there is a high overlap of merchants that offer both). However, 92% do not know their fraud rates in the mobile channel. 7% believe that mobile fraud is the same or lower than online fraud, while 1% believe that it’s higher. With such a large percentage that “don’t know,” it will be interesting to see how these results change as mobile becomes more of an established channel.

Size of Fraud Management Budgets
How much are online merchants spending to mitigate fraud risk? In 2011, survey results show that 25% of merchants spend 0.5% or more of their online revenues to manage online payment fraud, while 75% spend less than 0.5%. In 2011, across all merchants the median ratio of fraud management expense to sales was 0.1%. These spending estimates focus on the cost of managing fraud risk (internal and external systems and services, management development, and review staffing). Direct fraud loss (chargebacks, lost goods and associated shipping costs), as well as the opportunity cost associated with valid order rejection, are not included (see Chart #22).
**Budget Allocation**

For many years, merchants have consistently spent just over half their fraud management budgets on review staff, and 2011 was no different — on average, 52% was allocated to order review staff (see Chart #23).

<table>
<thead>
<tr>
<th>Internal Tools &amp; Systems</th>
<th>21%</th>
</tr>
</thead>
<tbody>
<tr>
<td>3rd Party Tools</td>
<td>27%</td>
</tr>
<tr>
<td>Oder Review Staff</td>
<td>52%</td>
</tr>
</tbody>
</table>

Only 18% of merchants reported that they would be increasing their staffing levels, as review staff costs remain the dominant cost driver of fraud operations. In terms of budget, over 80% reported that their budgets would remain flat or decrease in comparison to last year (see Chart #24).

**Expected Budget Change for Fraud Management 2012**

- **No Change**: 78%
- **Increase**: 19%
- **Decrease**: 4%

**Average % Spending Allocation for Fraud Management 2011**

- **3rd Party Tools**: 27%
- **Oder Review Staff**: 52%
- **Internal Tools & Systems**: 21%

**Top Priority Strategy/Area of Focus 2012**

<table>
<thead>
<tr>
<th>Outsourcing</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Analytics</td>
<td>18%</td>
</tr>
<tr>
<td>Automated Detection</td>
<td>55%</td>
</tr>
<tr>
<td>MR tasks/workflow</td>
<td>21%</td>
</tr>
</tbody>
</table>

Automated detection and outsourcing continues to be the most cited area for process improvement attention in 2012, followed by streamlining manual review (see Chart #25). Reducing the need for manual review and increasing the efficiency and effectiveness of reviewers is key to growing online business profits and managing the total cost of online payment fraud.

With such a heavy reliance on manual review coupled with continued online sales growth, order review teams will come under more pressure to review more orders in the same amount of time. Without the right tools and processes in place, orders in queue will become a growing concern. As department budgets remain tight, merchants will need to re-double their efforts to automate more of the fraud management process while keeping valid order conversion high and fraud loss low.

**BEST PRACTICE advice**

To optimize your fraud management operations, maximize automated order screening capabilities while streamlining workflow for your review team. Use a decisioning system where business users can create screening criteria based on order attributes, as well as results and information provided from a host of verification and validation services.

Look for portals where case management systems are seamlessly integrated with relevant third-party data sources. It’s imperative that reviewers access one consolidated tool rather than having to leverage multiple systems.

Finally, define and measure your key performance indicators throughout the fraud management lifecycle. Understand your performance baseline and objectives, so you can identify where you can fine-tune your fraud management operations. That which gets measured, gets improved.
Conclusion

To provide an overall assessment and basis of comparison, we took a snapshot of average merchant performance across four key performance indicators (KPIs): manual review rate, order rejection rate, percent of orders lost to fraud (Fraud Rate—by Order), and percent of revenue lost to fraud (Fraud Rate—by Revenue), as shown in Charts #26 and #27.

KPIs vary by merchant size and by industry. In general, the largest merchants tend to fare better. This may be driven by potentially more resources, tools and experience in combating online fraud, whereas smaller merchants may not have the resources at their disposal.

KPIs are more varied across industry, which is to be expected (note: Chart 27 does not reflect all of the industries cited by merchants). Each merchant is unique in terms of their business objectives, fraud tolerance and risk, which is reflected in the results shown in the charts.

Managing fraud is an ongoing balancing act where merchants constantly weigh tradeoffs among fraud loss, customer experience, and cost. If fraud is reduced, what happens to the number of rejected orders? Will good customers be impacted? If more orders are accepted, what happens to fraud, and how will manual review support this? Having a structured framework to address these tradeoffs can help merchants identify gaps and improve overall fraud management processes.
Resources & Solutions

To find information on CyberSource’s industry-leading fraud management solutions, self-paced webinars, and other whitepapers on electronic payment management, visit our online Resource Centers:

**Americas:** Visit www.cybersource.com. For sales assistance, call +1 888 330 2300 (international: +1 650 432 7350) or email sales@cybersource.com

**Latin America and the Caribbean (LAC):** For sales assistance, call +1 305 328 1998 or email lac@cybersource.com

**Europe | Middle East | Africa:** Visit www.cybersource.co.uk. For sales assistance, call +44 (0) 118 929 4840 or email uk@cybersource.com

**Asia Pacific:** For sales assistance, call +65 6671 5020 or email ap_enquiries@cybersource.com

**Japan:** Visit www.cybersource.co.jp. For sales assistance, call +81 (0) 3 3548 9873 or email sales@cybersource.co.jp

**China:** Visit www.cybersource.com/cn. For sales assistance, call +86 21 5116 7142 or +86 21 6109 5100, or email gc_enquiries@cybersource.com

**Australia & New Zealand:** Visit www.cybersource.com/anz. For sales assistance, call +65 6671 5020 or email anz_enquiries@cybersource.com

CyberSource Fraud Management Solutions

CyberSource’s industry-leading fraud management solutions enable businesses to detect fraud sooner and accurately, as well as streamline fraud management operations. With a hosted fraud management system and managed risk services that can supplement or manage complete portions of your review process, CyberSource provides flexible and powerful options that best meet your business needs.

CyberSource Decision Manager: Rule Console and Fraud Detectors

Having more data enables you to gain more insightful correlations to detect sophisticated fraud. Decision Manager is a hosted system providing access to a full range of data generated from global fraud detectors, multi-merchant and cross-industry correlations, truth data and more. Decision Manager comes with a business rule console that controls automated screening and case routing, an advanced case management system, and reporting and analytics.

Automatically screen more bookings up front, while providing your review team with access to fraud detectors and customized rules to help them review more orders, faster and more accurately.

Managed Risk Services

CyberSource Managed Risk Services enables you to scale your expertise and capacity without adding fixed headcount. Our staff of fraud analysts, review teams and chargeback experts stands ready to back your team, or even manage complete portions of your operation. All of our services are backed by business performance guarantees.

- Performance Monitoring provides supports for configuring rules and detectors, and monitoring process performance.
- Screening Management includes Performance Monitoring, plus our experienced review staff to manage manual order review per your policies. Available 24/7.

CyberSource Payment Management Solutions

In addition to our fraud management solutions, CyberSource offers a comprehensive portfolio of modular services and tools to help your business manage your entire payment pipeline to optimize sales results. All are available via one connection to our web-based services.

Global Payment Acceptance

Accept payments worldwide using a merchant account from your preferred provider: worldwide credit and debit cards, regional cards, direct debit, bank transfers, electronic checks and other payment types such as PayPal and Bill Me Later. CyberSource also provides professional services to help you integrate payment with front-end and back-office systems.

Payment Security

Remove payment data from your network, which is a great way to streamline PCI compliance and mitigate security risk.

- Payment Tokenization and Hosted Payment Acceptance Services: enables you to process payments without storing or even transmitting payment data.
- Payment System Centralization: Our team of experts will help you consolidate multiple payment systems into a single, easy to manage system. Link legacy systems to web-based services for rapid service expansion. Optionally, CyberSource will also host, support and manage these centralized payment systems in our secure datacenters.

Professional Services

CyberSource maintains a team of experienced payment consultants with proven systems integration expertise. Our client services team is additionally available to help you monitor, tune, or fully outsource portions of your payment operations.
About CyberSource

CyberSource, a wholly-owned subsidiary of Visa Inc., is a payment management company. Over 370,000 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 San Francisco and maintains offices throughout the world, with regional headquarters in Singapore (Asia Pacific); Tokyo (Japan), Miami/Sao Paulo (Latin America and the Caribbean), and Reading, U.K. (Europe/Middle East/Africa). CyberSource operates in Europe under agreement with Visa Europe. For more information, please visit www.cybersource.com.

AMERICAS
CyberSource HQ
Phone: +1 888 330 3200
    +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) 118 929 4840
Email: uk@cybersource.com

ASIA PACIFIC
CYBS Singapore Pte Ltd.
Phone: +65 6671 5020
Email: ap_enquiries@cybersource.com
www.cybersource.com/asiapacific

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

CYBS Greater China
Phone: +86 21 5116 7142 / +86 21 6109 5100
Fax: +86 21 5116 / +86 21 6109 5101
Email: gc_enquiries@cybersource.com
www.cybersource.com/cn

CyberSource Australia & New Zealand
Phone: +65 6671 5020
Email: anz_enquiries@cybersource.com
www.cybersource.com/anz

© CyberSource Corporation. All rights reserved.