2007 eCommerce Chargeback Report

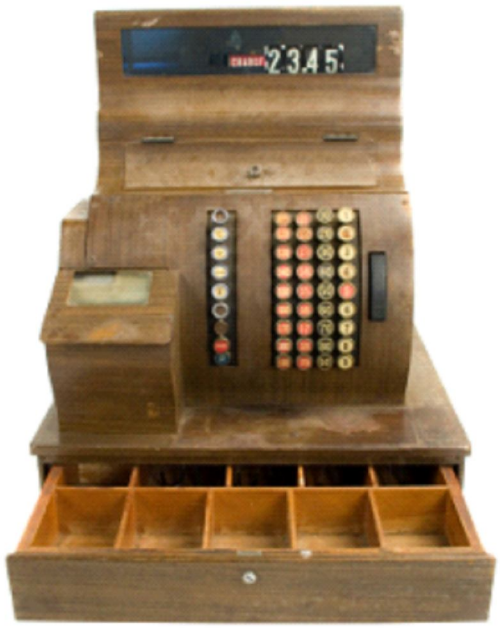
Is the real cost of fraud registering with merchants?

In This Issue:

Introduction

In an effort to give merchants a voice and to find out what's really going on in the marketplace from their viewpoint, nearly **2,000 global eCommerce merchants** were surveyed to create the first annual **eCommerce Chargeback Report**.

Based upon survey results, eCommerce transactions are expected to **increase 26% from 2006 to 2007**. As more businesses in more countries adopt eCommerce, transactions are expected to total **$8.45 Trillion** worldwide. This report provides a merchant–driven perspective that raises concerns about doing business online that, up until now, have not been uniformly presented and which are becoming increasingly problematic for merchants, limiting their revenues and increasing their costs.



Continued on page 2 ...

Report Methodology

A group of **1,950 qualified respondents** were chosen from a random sampling of webmasters, business owners and executives from various internet sources, including, but not limited to, preCharge merchants. The panel of merchants were invited by e-mail and the survey questions were provided by way of a web interface.

All respondents passed through a screening process that required panel members to be either owners or managers of eCommerce websites. In addition, the eCommerce businesses had to receive and process credit card transactions, and the members had to have direct knowledge of the entire order processing flowchart.

By surveying merchants who routinely deal with transactions and the risk of credit card fraud directly, this report presents information from a cross section of eCommerce merchants. The importance of obtaining data from a truly representative group of merchants cannot be underestimated.

Special Thanks

Our thanks go out to all the merchants who shared their time and information in order to respond to these questions.

Merchant911.org & Tom Mahoney - Through its network of merchants, Merchant911.org provided insight into the small and medium sized merchant user base to give a necessary perspective to create the **2007 eCommerce Chargeback Report**.

They are not all the same.

Comparing Apples and Oranges

Although it is easy to group all eCommerce merchants into one category and claim that eCommerce fraud is not a problem, the reality is quite different.

Certainly, if you are processing **$100 Million** or more every year, your perspective on fraud may be very different from that of the traditional "mom and pop" business processing **$10k or less per year**.

The largest concentration of revenue for **merchants in 2006** was seen in businesses processing **$10k to $100k per year online**, making up **32% of the overall** revenue stream.

Bottom Line

The eCommerce Chargeback Report confirms the effects of fraud, not just on major eCommerce sites, but on small and medium sized merchants as well, who are typically left with no voice.

Screening

Although **78% of merchants** surveyed reported a lower overall chargeback rate than previous years, an astounding **65% of merchants** surveyed stated that, unlike previous years, in an effort to curb chargeback rates, nearly **46% of chargebacks received in 2006** were given an automated refund, rather than suffering the downside of a chargeback. This was especially true for merchants processing less than **$5 Million per year**.

Staffing

Over **50% of merchants** surveyed reported having two or more full-time employees reviewing transactions on a daily basis, taking an average of **15 minutes per order** from start to finish. Equally as surprising, many merchants are finding that as manual review has increased, overall revenue has decreased significantly more than fraud rates have decreased, thus shrinking both bottom line and profitability.

Longevity

Of those surveyed, an overwhelming **69% of merchants** stated that their current business was at least their second online venture, and **32% reported** having had three or more previous ventures. As the Internet continues to mature, more and more merchants are maintaining their business operations longer and longer.

Please, Curb Your Fraud

Although transaction processing habits differed from merchant to merchant, the one constant was that nearly **95% of merchants** felt they could be doing more than they were to curb the cost of fraud and increase order activity.

Processing Time

The average processing time for an order depends heavily upon the backend tools used to verify the order. **89% of those surveyed** utilized at least one automated tool to verify orders, and a high percentage of merchants enlist manual review for almost every new order that is placed.

Screening Tools

Though merchants enlist both internal screening tools and third party solutions, they all can agree on one thing: fewer approved orders is bad business. Although each tool implemented has decreased fraud, they have also decreased their revenue.

A Happy Medium

Merchants market their products and services in a variety of ways, but they share two common goals: keep the fraud out and approve all the valid orders. Balancing these two goals proves quite difficult, especially for small to medium-sized merchants, as the majority of those surveyed felt a lack of industry support in combating this challenge.

Insult Rate

In an effort to reduce fraud losses, the bulk of online merchants are turning away orders more often than before. This not only ensures that customers will not return to shop again, but also that unhappy customers will spread the word.

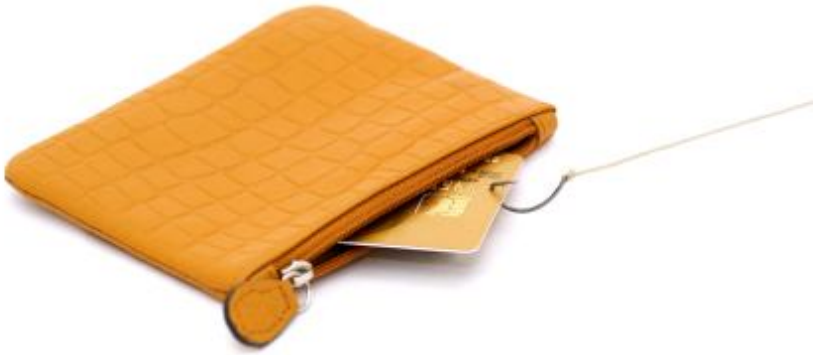
The Global Marketplace

Although **63% of those surveyed** have sold internationally, fewer than **15% actively sell internationally**; nevertheless, more than **85% of those surveyed** would actively sell internationally, if fraud could be managed properly.

While the jury is still out on whether domestic transactions are ultimately safer, respondents reported that at least **70% of chargebacks issued** were not international. While fear of fraud may be driving away business for most merchants, clearly, those taking the global plunge are reaping the rewards.

Bottom Line

Merchants are shrinking their current client base and missing out on global sales that could exponentially increase their revenues.



Are transactions really safe?

"Friendly" Fraud?

"Friendly" chargebacks are those in which the actual cardholder has, in fact, placed the order, but later denies having placed or received the order, and issues a chargeback. This ultimately results in merchants having to accept full responsibility, not only for the cost of the merchandise and/or services, but also the bank fees themselves, as consumers become aware of this loophole in the credit card industry.

Friendly chargebacks can happen for a variety of reasons, including buyer's remorse, non-receipt of merchandise, or simply non– recognition of the charges.

Even though a majority of merchants have experienced friendly chargebacks, the only solution they have come up with is manual intervention, by calling each client personally. However, that has not proven to reduce much of anything, except productivity.

The credit and debit card industry has been making it increasingly easier for consumers to file chargeback claims, and merchants have been given little, if any, industry support. Merchants continue to hope for an automated, unobtrusive way of determining whether a consumer is a likely candidate for friendly fraud. Until this need is met, merchants will continue to approve orders strictly, and can expect friendly chargebacks to increase because of the ease of consumer filing methods.

Is the Customer Always Right?

Although many of the chargeback reason codes claim to explain the situation as being the merchant's fault, figures have shown that this is merely one side of the story. An overwhelming **96% of merchants** have claimed that they have been wronged by friendly fraud at least once in the past **12 months**, and **50% of merchants** expect it to happen many more times as their sales and online presence grow. Because the majority of consumers win friendly chargeback disputes, merchants have accepted friendly chargebacks as a cost of doing business.

Bottom Line

Although it's a taboo subject in the transaction processing industry, "friendly" fraud remains a growing concern in the chargeback world. Merchants report that "friendly" fraud is on the rise, and there seems to be no end in sight.

Consumer eConfidence

Traditionally, consumer confidence is defined as the degree of optimism about the state of the economy that consumers are expressing through their saving and spending activities. Consumer eConfidence is a cross-reference between the degree of trust a consumer has in a website or business and the perceived level of security that must be present on the website before the consumer will share any personal information. As consumers turn to larger and larger merchants in the belief that their data is safer, the reality is that the bulk of breached data ultimately stems from larger merchants.

Conversion Rates

Based on eCommerce conversion rates, merchants saw a decrease in sales by as much as **30% from the previous year**. Merchants have overwhelmingly attributed this to a lack of consumer confidence, increased consumer information requirements, and validation during the order process.

Identity Theft

More than **60% of merchants** surveyed felt that consumers' fear of identity theft was the single greatest cause of order abandonment. Over **90% of merchants** with annual revenues of **$5 Million** or less fear that if consumers' concerns over identity theft are not addressed, sales will decrease in the upcoming year, especially as reported identity theft cases continue to rise.

Common Security Flaws

The growing trend in the merchant's line of thinking is that the more information asked of customers, the greater the assurance that orders are valid. In today's age of identity theft and declining consumer eConfidence, however, consumers don't want to share their personal information. In fact, they want to share as little information as possible, in order to be assured that they will not experience identity theft.

Bottom Line

Consumer eConfidence is a two-way street: consumers trusting merchants and merchants trusting consumers. Consumers want a quick and easy checkout process, but most merchants think that will increase fraud.

What direction are merchants headed?

Looking for Options

Across the board, a recurring theme was that despite new and emerging technologies, merchants were spending more and more time processing each order. Even though all the norms are in place, such as AVS (Address Verification Service), traditional manual review and even consumer validation through various means, the message has been heard loud and clear: merchants have been trying to find better ways to process orders. So why the increase in processing time?

While eCommerce saturation reached all time highs in the United States, international transactions, once part of the promise of global ecommerce, have become one of the largest, yet most fatal arenas for online merchants today. Currently there is no true standard for processing international transactions. Nearly **70% of merchants** simply do not accept international transactions due to fears of fraud. While the numbers are unclear, because nearly **65% of those surveyed** do not even track, or accept the possibility of, international orders, the message is clear that more revenue is being turned away than is accepted.

Bottom Line

While many options continue to come and go, it's clear that merchants are finding new ways to get consumers to spend more money on their sites. Although these options may sometimes seem confusing, there is no doubt that more options allow for additional streams of clients. However, many merchants continue to find that these additional choices may not generate enough revenue to justify the increased expense associated with integration, screening and, ultimately, fraud .

Nearly **90% of merchants saw 2006 as the year of Mobile Payments, Gift Cards and Third Party Payment options.** Gift cards continue to be one of the fastest growing payment sectors, yet very few solutions exist today to manage fraud brought on by these types of payment options. Because it is usually hard to distinguish traditional credit cards from gift cards, merchants are left to turn away otherwise valid orders for the simple reason that AVS was not designed to handle gift cards.

Third party payment services also continue to grow at astonishing rates, as consumers feel a lack of confidence in storing their personal information with multiple online merchants. As consumers continue to be drawn in by the lure of security, merchants are once again left holding the bag as third party payment processors do not want to be stuck with fraud and chargebacks. Due to lack of industry support, merchants continue to be hindered by a sector which should actually be a point of growth.

Sealing Merchants' Fate

At one time, merchants had to undergo rigorous review to qualify for a third party seal of approval. Today, the "seal of approval" has become nothing more than another commodity bought and sold online with a major credit card.

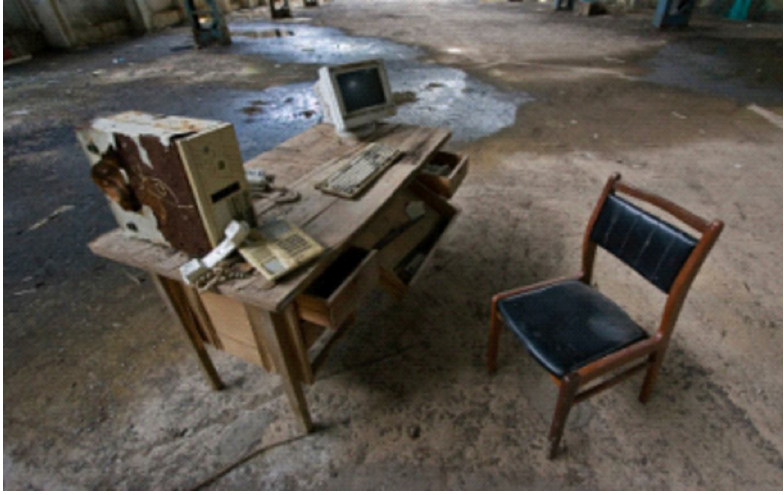
Are "seal" programs building a false foundation for merchant security? What happens when this foundation cracks, or worse---crumbles? While "seal" programs continue to be all the rage, in an alarming result, nearly **15% of those surveyed** utilized third party scanning programs offered by some "seal" providers as their only means of security protection when, in fact, these programs offered nothing more than daily, weekly or even just quarterly scans of a front-end website.

While industry regulations and state and federal laws are still emerging in this field, associations have continued to push certification on the belief that "would-be" certified merchants would not otherwise be liable for data breaches.

Although many "seal" programs promise certification with a simple scan of a website, the reality is that industry certification includes much more than just front-end security. Industry level certification actually encompasses many requirements otherwise unknown to merchants. As consumer confidence reaches new lows, many merchants unable to handle the increasing cost of managing security will continue to flock to cheap one-off solutions to give a certification that otherwise may not exist.

Bottom Line

As merchants continue to look for new ways to build their foundation, new offerings from the industry continue to allow merchants to find quick and easy ways to get certified. But are they working? While these seals are popular, they inexpensively validate security on what's typically nothing more than a handshake and a wink. Is this really what the industry needs?



Some things are worse than chargebacks.

Order Abandonment

Before merchants can pin down the true causes of shopping cart abandonment, the industry needs to take a serious look at building stronger consumer confidence. As major online retailers continue to treat the order process as a science, small merchants continue to see consumers abandon their order process before the final sale is completed. When asked why, nearly **70% of those surveyed** were unclear as to the reason.

Although talks continue to center on consumer confidence, very little discussion has addressed merchant confidence. Yet, **nearly 60%** of those surveyed felt a lack of confidence in their "merchant industry" relationships, such as processors, gateways and service providers.

Feeling The Pain

Of those surveyed, **only 3% reported** some form of **data breach in 2006**, yet the industry focus continues to be small businesses. Of the merchants **breached in 2006**, almost every one generated revenues in excess of **$5 Million** per year. So if big retailers are creating the problem, then why are smaller merchants forced to cough up greater percentages of their bottom line to building consumer confidence? When asked, "What are your plans for building consumer confidence in 2007?" nearly all merchants surveyed reported "nothing."

As consumer-based web technologies continue to hit the marketplace at an increasing pace, technologies geared toward merchants have become more and more scarce. Fewer and fewer technologies continue to become available to merchants, partly due to business focus on consumer-based services and partly due to the increasing cost to operate any merchant level service providers.

Bottom Line

Lack of consumer confidence is the single greatest threat to eCommerce ever seen. Merchants continue to look for new ways to build a confidence level, but can smaller merchants turn online confidence around?

PCI Compliance

PCI DSS stands for Payment Card Industry Data Security Standard, typically referred to as PCI compliance. The program consists of **12 requirements** including, but not limited to, security management, operational policies, security procedures, network architecture and software development. The program is currently overseen by the PCI Security Standards Council through a joint venture with American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International.

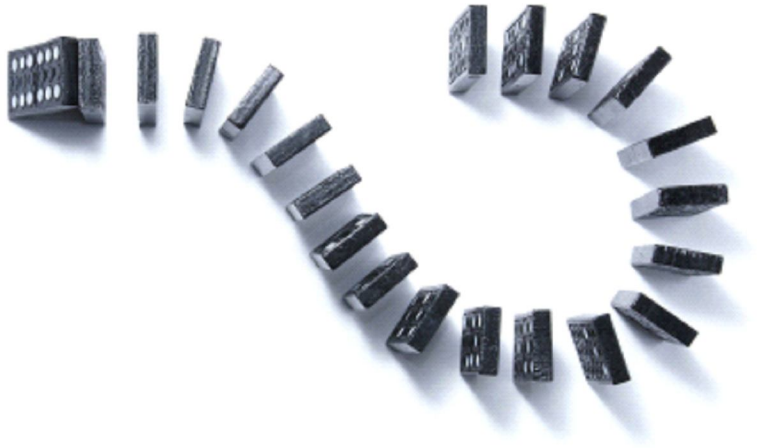
Understanding PCI Compliance

Currently, two separate programs exist under the PCI compliance program. One target merchants at four separate levels, each of which bears its own guidelines, ranging from quarterly scans to annual onsite audits. **71% of those surveyed** were unfamiliar with the various policies and procedures related to the program, and of the **43% of merchants** who are compliant, an astounding **92% of merchants** relied on third parties as a means of maintaining their required compliance.

Merchant Level Compliance, the second portion of the PCI compliance program, relates to service providers. This includes any third party who engages in the business of processing transactions for other merchants. Although industry regulations require merchants to utilize PCI compliant service providers, **72% of those surveyed** were unaware of a service provider level certification, and **85% of those surveyed** were unsure of their service providers' compliance with the PCI program.

Bottom Line

Of those surveyed, nearly 92% reported little or no knowledge of current PCI rules. This is certainly an alarming number, considering the industry push for merchant level certification.



Creating an uncertain future.

Creating A Domino Effect?

If merchants' confusion regarding compliance regulations is the biggest barrier to merchant level compliance, then why do industry regulators continue to impose new and ever increasing rules surrounding compliance?

Non-Compliance Vs. Security

Industry regulators have defined a compliant merchant as a secure merchant, but do eCommerce merchants say something else? Although only **3% of those surveyed** reported a **data breach in 2006**, nearly every one of them was compliant.

Merchant Confusion

If you give a man a fish, he will eat for one day, but if you *teach* a man to fish he will eat for a lifetime. While this old saying may seem like "common sense" to most, merchants continue to lack education about how to protect themselves against data breaches. Of those surveyed, **nearly 70%** felt that current security requirements imposed by the industry will do nothing to educate merchants on how to better protect consumer data.

Conclusion

eCommerce fraud will cost businesses **$9.25 billion in 2007** but, in reality, **the cost of managing fraud exceeds the cost of fraud itself by as much as 300%**. Despite lower than expected performance rates, merchants feel that they are forced to spend money on in-house fraud management because of the lack of effective third-party solutions to help them combat this problem. In an attempt to control fraud, merchants are also losing revenue from enforcing stricter controls on order acceptance, declination rates, rejection rates, order abandonment, shopping cart abandonment and the lack of confidence in accepting international transactions. While merchants overwhelmingly believe that eCommerce will continue to grow for many years to come, the fact is that the average spending per customer is steadily decline, thus causing even greater fears for eCommerce Merchants.

Merchants clearly need better tools, consistent guidelines and competent help to effectively manage online fraud and realize the full potential of safe, secure and cost-effective business online.

about preCharge

- **preCharge Worldwide**
  Toll Free (877) 751-6213
  Direct (212) 751-6213
- **preCharge Australia**
  Direct +61-290371912
- **preCharge Brazil**
  Direct +55-2137240749
- **preCharge Canada**
  Direct (647) 724-0626
- **preCharge China**
  Direct +86-21-5107-8454
- **preCharge Mexico**
  Direct (52) 55-2789-5391
- **preCharge UK**
  Toll Free (800) 047-0951
  Direct (44) 20-81146158

Founded in 2003, preCharge Risk Management has become a global leader in risk management tools designed to give merchants the resources necessary to do business anywhere in the world. With a global network spanning over **180 countries** and over **5 billion points of data**, preCharge maintains one of the most powerful networks and the largest fraud database on the planet, linking payment networks, gateways and merchants on a scale never before achieved.

preCharge is headquartered in New York City, New York with sales efforts throughout The Americas, The United Kingdom, Asia, and Australia.

preCharge Risk Management Solutions

130 7th Avenue, Suite 129
New York, New York 10011