MULTICHANNEL MERCHANT

Sponsored by

MELISSA DATA
Your Partner in Data Quality

A Call to Action for Merchants: Fight Fraud

BY ERIN LYNCH

As more shoppers are making their purchases globally and consumers are demanding faster shipping times, the threat of fraud for both consumers and retailers is growing rapidly.

The ThreatMetrix 2012 State of Cybercrime study, which was conducted among U.S.-based financial and retail business managers and IT executives, found that Trojan horse and phishing attacks were the most common cyberthreats for retailers. Forty-five percent of retailers said they had experienced at least one malware attack in the past year, and 45% had experienced at least one Trojan horse attack.

Despite acknowledging that they are experiencing cyberattacks, very few retailers are spending quality time researching security threats in order to stay one-step ahead of cybercriminals. Forty-seven percent of those surveyed were spending less than five hours each month on security research, and 14% were spending no time at all on preventive research.

But retailers that fail to improve their online fraud and cybercrime prevention practices put themselves at risk of both lost revenue and a damaged reputation as customers react.

60% of large retailers, 64% of mobile retailers and 74% of international retailers are affected by fraud.

The Cost of Fraud

The National Retail Federation estimates that nearly $9 billion was lost by merchants in returns fraud in 2012. And according to the ThreatMetrix report, online fraud resulted in about $3.5 billion in lost revenue in North America last year. Which makes it imperative, now more than ever, that retailers to step up and strengthen their cybersecurity.

According to the LexisNexis 2012 The Cost of Fraud study, retailers in 2011 were paying, on average, $2.30 per every $1 lost in fraud. In 2012, retailers paid $2.70 for every $1 lost. The study also found that for mobile retailers, the cost is even higher. In 2012, mobile merchants paid $2.83 for every $1 lost, compared to just $2 in 2011. The increase, according to the study, is due to several factors, including the impact of lost and/or stolen merchandise on the company's bottom line and post-fraud costs from customer attrition.

(LexisNexis defined fraud as fraudulent/unauthorized transactions, fraudulent requests for a refund/returned or bounced checks, lost or stolen merchandise, and redistribution costs associated with redelivering purchased items.)

When fraud happens at an ecommerce company, the costs are more than financial. If your security is breached in any fashion, customers will become wary about shopping with you and about sharing their personal information, such as credit card data and email addresses. Not only are you losing sales, but there goes your hand-raiser for marketing purposes.

In fact, according to recent statistics, one out of every three consumer fraud victims will change where they shop based on being a victim of fraud while shopping online.

Alternative Payments

As technology grows, so do the various ways shoppers can pay for a purchase online. Gone are the days when consumers used the standard major credit cards such as MasterCard, Visa and American Express. This is true with American shoppers and retailers, and also true across the globe.

Even though major credit cards and PayPal have become the standard for most American shoppers, international shoppers are looking for a more localized payment experience. In Africa, shoppers want to pay through a mobile device called M-Pesa. In South America, an emerging market for online shopping, consumers are hesitant to reveal their credit card information while buying or purchasing products online and are looking for additional payment options in order to complete their purchases.

According to the 2013 MCM Outlook Report, when respondents were asked what type of alternative payment options they provide on their websites, the number-one response was PayPal (40%), followed by gift cards (25%), Bill Me Later (16%), Google Checkout (9%), Amazon Payments (8%) and eBill Me (3%); 5.1% said "other."

Nearly 42% of respondents said they do not use an alternative payment option on their sites. That could be because these new payment options are opening the door a little bit wider for fraudsters to gain access to user accounts and information.

Who Is Most Affected by Fraud

While no single ecommerce site is immune to fraud, studies are showing that there are higher risks depending on the scale of your business. The LexisNexis study found that 54% of all retailers are affected by fraud. Broken down even further, the study found that 60% of large retailers, 64% of mobile retailers and 74% of inter-

national retailers are affected by fraud.

In fact, according to CyberSource Corp., an electronic payment and risk management provider, international orders are more than three times as likely to be fraudulent as domestic orders.

Translation: There are two types of retailers in the ecommerce world, those who have been affected by fraud and those who will be affected by fraud. So, it's bound to happen at your company one way or another.

Fraud-Fighting Technologies

According to the LexisNexis study, merchants are beginning to focus on adopting fraud-fighting technologies, such as device fingerprinting, IP geolocation, automated transaction scoring, and real-time transaction-tracking tools. However, there is still room for improvement for larger ecommerce companies.

The LexisNexis study found that 15% of large ecommerce companies use device ID/device finger-printing solutions, 22% use automated transaction scoring, 29% use IP geolocations, 30% use real-time transaction trafficking tools, 32% use rules-based filters, 38% have transaction/customer profile databases, 54% have card-verification tools (such as CVC or CVV1), and 55% use transaction verification/validation services.

According to the study, several of the above mentioned tools "are particularly" useful when applied to mobile shopping channels as well.

When merchants who sell internationally were asked in the LexisNexis study to name their most effective tools for controlling fraud, the top-five responses were:

- Card verification value software (32%)
- Pin/signature authentication software (31%)
- Transaction verification/transaction validation services (27%)
- Authentication of transaction/3-D secure tools (24%)
- Check verification services (21%)

Quick Facts About Fraud**

- **5.26%** of U.S. adults were affected by identify fraud in 2012
- **1 in 4** data breach notification recipients became a victim of identity fraud in 2012.
- Incidents of identity fraud impacted **1 million more** consumers in 2012 than 2011
- The dollar amount stolen increased to **$21 billion** in 2012.
- Merchants and banks absorbed the bulk of the costs of fraud

**Source Kount blogpost: Hacking Away Your Bottom Line

In addition, 18% named address verification services and 18% cited IP geolocation services.

Fraud management tools have several benefits, according to a whitepaper by FirstData. For example, they allow merchants to quickly adjust their scoring and resolution parameters in order to optimize results for their ever-changing business needs; they reduce staff time spent on manual order reviews; they can allow a company to stay up to date with the latest fraud protection tactics; and they can reduce chargeback costs.

Best Practices in Combating Fraud

Many retailers are taking steps to prevent fraud on their sites, according to the 2013 MCM Outlook Report. Sixty percent of the respondents said their sites include a trustmark of approval from a third-party company, 29% did not, and 11% were considering it.

Of those who responded that they use trustmarks, the top-three most popular were SSL security, Verisign and McAffee.

While trustmarks are a way to make shoppers feel comfortable sharing information and shopping with your ecommerce company, retailers need to feel just as safe when accepting transactions. Unfortunately, fraud protection doesn't seem to be a major focus with retailers. Although a new study by ThreatMetrix found that 85% of retailers are calling cybersecurity a high priority within their organizations, 40% of the respondents said they have no online prevention measures in place.

Here are a few steps you can take right now to improve fraud detection and combat fraud on your retail site:

Display fraud notices. Balistic Merchant Services recommends that merchants place fraud notices on their sites and order forms which, they say, "deter most online scammers." These notices, according to the payment processing service provider, should also include that violators will be pursued to the full extent of the law, and can be tracked by their IP, email addresses, etc.

Get a fraud-screening system in place. More and more retailers are using fraud-

screening systems that identify potentially fraudulent transactions. Quality systems, according to WorldPay, compare the payment information that your customer supplies with a constantly updated database of millions of payments. Screening programs will help a retailer detect patterns of fraudulent activity and potentially fraudulent situations.

Fraud-screening systems could, ultimately, lower costs within your organization, reduce the rate of online fraud, lower the legitimate purchases you turn down, customize your own security checks, and keep your site up to date on the latest security threats trolling the web.

Gather as much data as possible on every transaction, no matter how trivial it may seem. Using a broad dataset will help retailers apply a statistical approach to the data and create an analytical model that can help fight against fraud.

Conduct a manual review of transactions. Take the following steps in an attempt to authenticate a purchase: Look into the customer's previous transaction history, contact the customer directly to verify identity, and/or use Google Maps or IP geolocations to verify delivery addresses.

Have clear and articulate terms and conditions on your site. Make sure your shopper acknowledges these terms before a purchase to minimize chargebacks. This should be followed by a confirmation email or online order validation that requires some sort of customer action.

Get card verification numbers and expiration dates. BMS states that obtaining the three- or four-digit verification codes and expiration dates found on most major credit cards is another step you can take to ensure that the credit card is actually in the hands of the shopper.

Send an email to your customer after a purchase. One of the best practices when working with your shopper, regardless of fraud or not, is to send an email to the address provided with a link to activate an account or order. But when it comes to a questionable purchase, the move could block a "fraudster" from verifying a fraudulent purchase and will also give you a history trail of the shopper if the consumer wants to dispute a transaction later.

By creating a balance between your internal fraud safeguards and how you manage the customer experience, you should be able to maximize legitimate revenue while fighting fraud on your site. Currently there are hundreds, if not thousands, of payment processor and fraud risk management vendors out there willing to assist your company combat fraud if you feel it cannot be done internally.

Strategies for Loss Prevention Risk Management

More retailers are learning that if they want to combat losses ranging from online and returns fraud to data-related losses within their businesses, they need to create and analyze real-time data. That step is essential to staying one step ahead of recurring shrink. Studies have also shown that retailers who use loss prevention risk management strategies see a reduction in fraud-related and operational costs.

The first step to any loss prevention strategy is to get your company's centralized loss department involved. Even though 16% of the companies surveyed in the Aberdeen Group's The State of Loss Prevention in Retail: Controlling Losses and Maximizing Profits found it beneficial to deploy loss prevention teams at every store, 40% of retailers said they were allocating regional loss prevention managers across multiple stores.

Realizing the power that business intelligence offers an enterprise, smart retailers are ready to exploit the power of analytical platforms to improve their loss propositions. The Aberdeen study found that 49% of retailers are successfully applying the results they learn to control their loss levels.

Every successful major retailer is using analytics within its organization, and this should be no different when it comes to loss prevention. By looking into analytics, reporting tools or smart tracking solutions, retailers will be able to make a positive impact on their bottom line.

The following MULTICHANNEL MERCHANT articles by staff and industry experts were sourced for this executive research summary. Please click on the article titles to learn more:

- 3 Ways to Protect Your Customers During the Holiday Rush
- NRF Says Return Fraud Could Cost Retailers $2.9 Billion This Holiday Season
- 3 Strategies for Loss Prevention Risk Management
- Best Practices in Combating Fraud
- How Retailers Can Fight Fraud
- Study Finds 40% of Retailers Do Not Have Online Fraud Prevention in Place
- More Payment Options Will Increase Global Sales Online
- Returns Fraud Hurting Online Retailers
- Fraud Management Tools Have Several Benefits
- Quick Facts About Fraud