

ROADMAP TO »

Online Fraud Prevention

RETAILERS USE SUITE OF TOOLS TO REDUCE FRAUD AND FALSE POSITIVES

BY DORI SALTZMAN

»» THOUGH THE PERCENTAGE OF REVENUE LOST BY RETAILERS TO ONLINE

fraud has gone down since 2000, the dollar amount lost has almost doubled. According to the MRC Platinum Fraud Survey conducted by the Merchant Risk Counsel, in 2000 the percent of revenue lost to online fraud was 3.6 percent and the dollar amount lost was \$1.5 billion. In 2006, the percent lost was only 1.4 percent, but the dollar amount had risen to \$3.0 billion. As retailers continue to grow their online business, their risk of losing even greater amounts is growing as well.

» WHAT IT MEANS

The frightening thing about online fraud is that it's really quite easy. All anyone needs to perpetuate fraud online is a valid credit card number. Valid numbers can be obtained many ways including identify theft, credit card skimming and advanced software that generates valid numbers and checks them against actual accounts. Regardless of how criminals get a valid number, once they have one they're going to try and hit online retailers for as much as they can get. Once a fraudulent order has been processed, shipped, noticed and reported, the retailer is held completely accountable.



Aersoles reduced online fraud by implementing online credit card authorization.

Preventing online fraud requires a mix of tools each designed to identify and combat different aspects of online fraud.

According to the Merchant Risk Council survey the average number of tools used by retailers is 4.8, with the most common tools used being an address verification service (79 percent) and a card verification number (69 percent). Other tools commonly used are automated decision/order screen systems (30 percent), IP geolocation services (35 percent), order velocity monitoring (33 percent) and address point verification systems (37 percent).

» WHAT'S AT STAKE

According to the MRC Platinum Fraud Survey, the average percent of all accepted orders that actually result in fraud is only 1.1 percent. But when slightly over one percent can cost a retailer millions of dollars, even one percent is too much. Sixty-five percent of fraudulent orders result in credits being issued by the retailer (this includes chargebacks initiated by the retailer as opposed to those initiated by a credit card company). In these cases, the retailer loses the product shipped, as well as the cost of the product, probably pays a penal-

ty to the credit card for the chargeback and also absorbs administrative costs incurred during the processing of the refund.

By implementing a cocktail of fraud prevention methods retailers reduce the costs associated with fraud by stopping fraudulent orders before they are processed. In addition, retailers can actually increase sales by safely allowing more transactions and improve customer satisfaction by reducing the number of legitimate orders that are delayed or declined. Legitimate orders that are delayed or declined due to suspicion of fraud are called “false positives.”

Rejecting legitimate orders because they may appear fraudulent, and losing customer loyalty because of rejected orders, is a very real risk to online merchants. The Merchant Risk Survey found that 4.1 percent of all orders placed with online retailers are automatically rejected because of suspicion of fraud. Many of these rejections may in fact be “false positives.”

Using a combination of fraud prevention methods to create a series of more complicated order rejection rules is one way to limit the number of orders rejected as fraudulent. Another way of limiting the impact of “false positives” is to set up rules that flag suspicious orders but don't

necessarily reject them out of hand. Manual reviews can then be done to verify that orders are in fact valid.

HOW TO SUCCEED

One retailer using a fraud prevention tool to help identify “good guy” orders is Abe's of Maine, a cross-channel consumer electronics retailer. Abe's uses a system from TARGUSInfo, an address verification service, to verify 98 percent of all orders, allowing more valid sales to go through. TARGUS “helps us verify orders that we might have rejected,” says Abe Mosseri, owner of Abe's of Maine. “We actually process orders that we would have possibly been uncomfortable with before.” Such orders include large orders with express delivery and orders with different bill to/ship to addresses.

Overstock.com, a “pure play” Internet retailer, uses the FraudNet system from The 41st Parameter to combat fraud without impacting the shopping experience of its customers. “Creating a superior experience for customers is a critical priority for Overstock.com,” says Stormy D. Simon, senior vice president of branding and customer care at Overstock. The e-tailer does not want its customers to be slowed down or delayed in anyway during the checkout process. FraudNet provides Overstock with “ex-

cellent anti-fraud capabilities while maintaining a seamless online shopping session for our customers.”

A key element of a successful online fraud prevention program is flexibility. All retailers are not the same, and neither are their customers. Business rules that apply to one may not apply to another. While certain best practice rules are applicable to most retailers, being able to customize fraud screens and rules is essential. Footwear retailer Aerosoles uses a fraud prevention and detection module offered by its e-commerce vendor Ignify to weed out fraudulent orders. “It was important to us to have the ability to set various levels of fraud protection on the site,” says Magnus Gustafsson, vice president of direct marketing at Aerosoles. The module allows Aerosoles to set its own rules, in addition to the best practice industry rules offered as part of the module.

Aerosoles also added online credit card authorizations to its recently relaunched site. Prior to the deployment of online authorization, the lag time between the processing of an order and the authorization of a credit card allowed more fraudulent orders to go through. “Now because of the authorization,” says Gustafsson, “if there is a fraud we can detect it right away and stop the order.” **RIS**