



Holiday Fraud On the Upswing

Sophisticated Schemes Are Cropping Up— In Store and Online

By Julie Ritzer Ross

The holiday season may bring increased sales volume for merchants and growing revenues for independent sales organizations (ISO), but it also will bestow another gift in the form of heightened fraudulent activity.

“Between the lackluster economy tempting people to commit fraud to fund their shopping and the growing ease of access to massive volumes of credit card information, there’s no question” that industry players “must prepare for more hits,” says Randy Lobban, director of risk management at North American Bancard.

E-commerce is expected to take a particularly hard hit, according to a survey by CyberSource, a provider of electronic payment and risk management solutions. The survey indicates that dollar losses from e-commerce fraud continue to grow, with fraudsters expected to divert approximately \$3.6 billion from U.S. e-commerce in 2007, a 20 percent increase over 2006. Not surprisingly, the period from Black Friday (the day after Thanksgiving) to December 25 is the most significant hotbed of such activity.

Additionally, the survey shows, 27 percent of online orders were manually reviewed in 2007. “The number of orders requiring manual processing (due to their suspicious nature) is growing faster than online sales, which are increasing by about 20 percent annually,” the survey says. Approximately 38 percent more orders were reviewed in 2007 than in 2006, CyberSource estimates.

“E-commerce in the U.S. today is a highly rewarding channel that is showing vigorous growth,” says Doug Schwegman, CyberSource director of customer and market intelligence. “But it’s also a channel with meaningful challenges posed by systematic

fraud. Merchants did see their online sales grow approximately 20 percent, but the costs of managing fraud grew a nearly identical amount. The picture is one of merchants swimming harder against an accelerating current.”

Casting A Wider Net

In the past, thieves may have been content to steal a single credit card number, but technology makes it easier to do more damage in less time. “In the Internet age, fraudsters can obtain giant files of credit card data and then sell it on the Internet to get more,” Lobban says. “They can go to malls where stores have upgraded to wireless networks but have neglected to upgrade their encryption technology, and snatch files en masse.”

They can hack into merchant accounts and re-program terminals to make transactions look legitimate, reports Tom Dunn, president of TriSource Solutions. “Even if the amount of fraud we’re seeing at holiday time in brick-and-mortar stores remains relatively unchanged, the tech-sophistication is ramping things up on the online side,” he points out.

Adding insult to injury, a number of seemingly complex schemes are surfacing. In one such scheme, stolen credit card numbers are used not only just to purchase goods and services, but also to fund gift cards. In another, a “customer” whose card is rejected at the point-of-sale tells a store associate that he or she will telephone the issuer for an authorization. When the call is answered, the fraudster hands the phone to the store associate, who, instead of being on the line with a representative for the issue, is really speaking with the “shopper’s” accomplice.

Cyber-schemes are comparably sophisticated. For example, cyber crooks will

choose the “hot” toy or other popular product of the holiday season and send out an e-mail blast advertising it for sale at a much lower price than it typically sells for. Victims who fall for this ruse end up entering credit card information on malicious sites designed to look like legitimate online stores. They might also unknowingly download a “keylogger” that can steal personal information entered when completing an e-commerce transaction.

In addition, hackers have begun to inject code into Web pages to redirect users from legitimate e-commerce sites to bogus ones in the hope of capturing credit card numbers and other data. The Web site of Dolphin Stadium in Miami was attacked in this manner prior to the 2007 Super Bowl.

Emphasizing Best Practices

Although sources declined to discuss their own procedures for helping merchants grapple with fraud during the upcoming season, they say ISOs can—and should—remind merchants not to allow the increased volume of business they ring up at holiday time distract them from exercising best practices aimed at minimizing fraud. “Merchants see any input they receive from acquirers and ISOs on this front as a service, so it not only helps to control fraud, it acts as a value-add that makes for a better business relationship going forward,” says Vicki Strayer, vice president, enterprise business compliance, TSYS Acquiring Solutions.

According to Strayer, merchants should be urged to review their holiday sales projections and adjust the parameters of any risk management software they may have in place to add a layer of transaction-monitoring vigilance. Lobban agrees, adding that

North American Bancard offers a service to its merchant customers wherein its risk management department will, in certain cases, conduct pre-authorizations of unusually large, possibly suspect sales.

"We would rather be notified in advance of a situation like this rather than get an angry phone call about it later on," he says.

Best practices for brick-and-mortar stores include comparing the signature on the card with the signature on the receipt or electronic signature capture device, as well as refusing to allow a customer attempting to execute a suspicious transaction (for example, one that may involve a stolen card) to initiate a telephone call to an issuer and hand the receiver to a store clerk. "We advise our merchants to call the card issuer themselves, at the number they have on file, to be certain of whom they've reached, and only then to allow the shopper to get involved," Lobban says.

Additionally, North American Bancard counsels its merchants to ensure that they change the manufac-

turer's password provided with their point-of-sale and transaction processing systems. "They may forget such a step in the haste to get new software up and running before the holiday rush, but that can be a really costly mistake," Lobban notes.

Maintaining An Eagle Eye

Card-not-present transactions merit even closer scrutiny and best-practices application. ISOs would do well to caution merchants to consider as possibly fraudulent any unusually large orders placed through the Internet without any communication from the buyer. Rush orders for large quantities or high-priced goods need similar scrutiny. As one source points out, crooks may ask to have an order shipped overnight so they know exactly what day the order will arrive and can be waiting to pick it up. Other red flags include missing information such as a daytime phone number, requests for shipment of an order to an address different than the billing

address, orders from abroad, orders bound for foreign countries to be paid for with a U.S.-issued card and billing addresses that do not match the information on file with the issuer.

Considered individually, none of these factors are definitive indicators that a transaction is fraudulent. However, when several such signs are present, it's best to investigate the matter, Dunn says.

Dunn and others say the importance of using AVS or CV2 services (electronic notification services provided by most card issuers) to verify cardholder addresses cannot be over-emphasized, particularly during the holiday season. Encouraging merchants to implement fraud-detection tools that block suspicious transactions based on the point of origination or other factors also is not a bad idea, they say.

According to the CyberSource survey, 53 percent of merchants used five or more fraud-detection tools on their e-commerce sites in 2007, the largest merchants using an average of eight. **TT**