



Scanning the Card-Fraud Horizon

While vishing, phishing, and pharming persist, efforts to inform the public help keep fraud at bay

By Thomas Goldsmith

Now that that the pressure of the holiday retail season is in the rearview mirror, those who toil in the back office looking for (and intercepting) persistent—and sometimes ingenious—attempts at card fraud can take stock.

As always, there is good and bad news. Fraud attempts are still with us, of course, but consistent vigilance and an ever-increasing degree of cooperation and communication among the payments industry's fraud experts are doing a better-than-ever job of minimizing the number and size of such incidents.

Fraudulent transactions held steady in 2007 at about 2 percent of the total, the same as in 2006, according to Celent Communications, a banking industry consulting firm based in Boston. Most of that fraud originates from lost or stolen cards (48 percent), but identity theft (15 percent), skimming and cloning scams (14 percent), and counterfeiting (12 percent) still account for significant amounts of fraud.

For the details, there is no better source in the United States than the members of the Merchant Acquirers' Committee (MAC)—a group of risk-management professionals who keep a watchful eye on the scammers. The committee's primary purpose is to share information, says Deana Rich, MAC president and principal of Rich Consulting. MAC ensures news about fraud schemes directed at one institution or one industry segment is communicated to others who may be targeted.

Although "nothing terribly new" is going on with current fraud attempts, says Rich, one new variation on an old scheme is causing more than a few headaches for the payments industry. "Vishing" draws from the long-lived "phishing scams" that still show up in email in-boxes. Vishing involves a telephone call from someone claiming to be a security representative of one of the card issuers or card brands.

Typically, the caller alerts the consumer to an alleged suspicious charge on his or her card account (the caller usually has the card number) and asks for a confirmation that the charge is legitimate. When the consumer says the charge isn't valid, the caller then asks the consumer for the three-digit security code on the back of the card. Those who provide the code soon see truly bogus charges on their statements.

Vishing, phishing, and pharming (which relies on Web sites to swindle cardholder data) currently are the most persistent forms of fraud.

"I'm amazed sometimes that hundreds or even thousands of people still are being victimized, despite the publicity around these scams and the efforts to educate consumers," Rich says. She adds that MAC members also see a fairly steady amount of "skimming" in which thieves



use portable devices to scan and record magnetic stripe data from cards. It usually occurs at locations where consumers lose sight of their cards for a time, such as in restaurants.

Debit card fraud activity tops Rich's list of scams on the rise. To get authorized use of a debit card, the thief needs two pieces of information—generally the magnetic stripe data and a PIN number. Fake face plates on ATMs are frequently used to get the card stripe data, while cameras are strategically placed to record PIN numbers.

"We're also seeing a new run of 'zero-batch' transactions with debit cards," she adds. They're a variation of a tried-and-true scam developed with credit cards. In simple terms, a purchase made with one card is "returned," but the refund transaction is credited to a different card that is owned by the scammer. This kind of theft was relatively easy to trace with credit cards, but with debit cards, the refund can be converted quickly and easily to cash, which is essentially anonymous when it is spent.

Unfortunately, card fraud isn't likely to go away in spite of the surge of re-

Because the very nature of fraud prevention is a defensive game, acquirers are almost always going to be a step behind, reacting to whatever scam artists are clever enough to dream up next.

search and media attention paid to it, says Rich.

"We're always going to have some fraud, because of the way we live and use our credit and debit cards," she explains. "We want a transaction to be fast and convenient, even if that takes away the opportunity to thoroughly check transactions." And because the very nature of fraud prevention is a defensive game, acquirers are almost always going to be a step behind, reacting to whatever

scam artists are clever enough to dream up next. For the risk-management professionals, the premium is on reacting quickly and containing threats as soon as they're identified. "And we're getting better at that," she adds. **TT**

Thomas Goldsmith is ETA's director of communications and public relations. Reach him at thomas.goldsmith@electran.org. Contact Deana Rich at deana@dricbconsulting.com.



For more information or to get involved in MAC, contact: Laurie LeBoeuf, MAC vice president and Membership Committee chair, at lboeuf@tcbconsultingonline.com. MAC will hold its 2008 Annual Meeting March 19–21 in Las Vegas.

Tired of working for pennies?

Interested in offering your merchants a

FREE Service

that pays you \$9.00 per transaction?



Call Harry at (800) 208-2964
sales@checXchange.com