



## Lessons in 21st Century Crime

*Next-generation fraud prevention tools now stop increasingly high-tech cyber frauds in their tracks*

By Julie Ritzer Ross

**A**s online fraud surges, a thorough understanding of new tactics and defenses can help ISOs and processors position themselves as trusted merchant advisors, rather than mere products providers. Knowledgeable advice not only helps merchants keep fraudsters at bay, it acts as an ISO or processor's value-add and a point of differentiation.

Statistics tell the story: Online payment fraud accounted for 1.4 percent of online revenue—approximately \$3.6 billion—last year, according to a report released earlier this year by electronic payment and risk management solutions provider CyberSource. While credit card fraud as a percentage of total sales losses has trended downward since 2004, losses due to fraud are trending upward as more merchants—including small- to medium-sized players struggling to compete against their cyber-savvy counterparts—begin riding the Internet wave.

Moreover, online credit card fraud will continue to rise until 2010 at the earliest, according to the “2008 Identity Fraud Forecast” from research firm Javelin Strategy & Research in Pleasanton, California. Adding insult to injury, Javelin analysts quoted in the report said three out of 10 fraud victims have decreased their online shopping, and that the potential for online fraud makes many others uncomfortable doing business online.

“E-commerce in the United States today is a highly rewarding channel that is showing vigorous growth,” says Doug Schwegman, CyberSource’s 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 in 2007, but the costs of managing fraud grew by a nearly identical amount. The picture



is one of merchants swimming harder against an accelerating current.”

### More than ‘Phishing’

One notable trend is the evolution of cyber-scams and schemes from the simple to the highly complex.

For example, some savvy perpetrators now disseminate e-mail blasts advertising a popular item for sale at a greatly discounted price. 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 “key-loggers” that can steal personal information entered when completing e-commerce transactions.

In addition, hackers have devised means of injecting code into Web pages to redirect users from legitimate e-commerce sites to bogus ones in order to capture their credit card data. The Dolphin Stadium Web site was attacked in this manner prior to the 2007 Super Bowl.

“But these scams are really the tip of the iceberg,” notes David Montague, founder and president of The Fraud Practice, a New Jersey-based consulting firm that provides payment, fraud prevention, and credit-granting consulting services to clients in a variety of vertical markets. “Many others are coming to the surface.”

“Internet Protocol (IP) spoofing” is one example. IP spoofing takes advantage of the fact that cybercrime is less prevalent in some areas of the country, such as the Midwest, and more common in others, as well as in Eastern Europe and Western Africa. In IP spoofing scenarios, hackers route traffic through “botnets,” or networks of computers that forward spam, viruses, malware, and similar transmissions to other computers linked to the Internet. This occurs without the users’ knowledge and makes the IP addresses of perpetrators’ computers appear to be located in low-risk areas so as not to arouse merchants’ suspicions.

“Card generator fraud” is another hot scam. Here, cyber-criminals prey on small banks’ weaknesses, such as out-of-date AVS systems, and attempt to hit all the card numbers within that bank’s assigned credit card number range.

“Once fraudsters successfully receive an authorization from one of the credit card numbers, they will make purchases with it from one merchant and then another merchant if they can,” Montague explains.

In a somewhat different vein, other cyber-criminals are stealing credit card numbers online—often in chat rooms—and using them to buy gift cards. The cards are then redeemed for merchandise, which thieves resell to other merchants. Earlier this year, Montague reports, a Massachusetts man was arrested for allegedly having fraudulently obtained several hundred credit card numbers in Internet chat rooms and using them to buy more than \$100,000 worth of Dunkin’ Donuts gift cards. The man then used the gift cards to buy cartons of beverages, which he “fenced” to local delicatessens and bodegas.

“More and more of these schemes will undoubtedly surface as chip and PIN acceptance closes the door for cyber-criminals to commit e-commerce fraud outside the United States,” Montague predicts. “Merchants—and by extension, ISOs—are the low-hanging fruit.”

### Technology and Prevention

On the flip side, technology aimed at combating online payment fraud is rapidly evolving. Unlike previously available solutions, which attempt to identify fraudulent orders after the fact, next-generation applications stop perpetrators in their tracks.

For Craigslist and Google, among others, an aptly named solution called “telev verification” is the weapon of choice. The application prompts consumers for their telephone number when placing an order. An automated telephone call is then placed to that individual, who receives a unique security code via automated message or short-messaging ser-

## “Merchants—and by extension, ISOs—are the low-hanging fruit [for cyber-criminals].”

—David Montague, founder and president,  
The Fraud Practice

vice text messaging protocol (SMS). The code must be correctly entered into a designated place on the merchant’s Web site in order for the transaction to be successfully processed.

Sources point out that requiring the confirmation of a workable, traceable telephone number detracts criminals because they are wary of giving a legitimate phone number that can be traced back to them. Telev verification also is easily integrated into online merchants’ Web sites by adding a few lines of code to an existing site that will allow it to interact with a telev verification provider’s server.

Meanwhile, CyberSource has integrated information verification technology from TARGUSinfo into its Decision Manager solution. The program seeks and confirms matches between ordering parties’ names, addresses, and telephone information, including wireless, Voice over Internet Protocol, and other non-public phone numbers. Incoming orders are analyzed according to more than 150 integrated fraud detectors and merchant-specific business rules. If a transaction shows suspiciously high risk, the order can be rejected or queued for manual review.

Another player, ID Insight, recently unveiled Safe2Ship, a tool that utilizes its proprietary Access-Point Intelligence technology to search out fraudulent transactions prior to processing. Safe2Ship analyzes every available piece of information about a customer’s access points, including physical address, phone number, IP address, and e-mail address. Online merchants send in “bill-to” and “ship-to” addresses in real time or in batches. In about a second, the Safe2Ship engine examines hundreds

of address-related data points, searching for out-of-pattern shipping behavior. ID Insight’s patent-pending predictive analytics are then applied to determine the likelihood of fraud in a mismatch between the bill-to and ship-to address.

The Safe2Ship engine generates a risk score, which predicts the legitimacy of each address mismatch and the likelihood that a potential case of fraud is underway. Merchants may adjust risk tolerance as business factors change.

“From what we have seen, there has been a shift in technology wish-lists for combating online credit card fraud to those that minimize the number of cases that must be reviewed manually,” says ID Insight President Adam Elliot.

The Merchant Risk Council (MRC), a trade association for preventing online fraud and promoting secure e-commerce, recommends cyber-merchants incorporate Trustwave’s Extended Validation SSL (Secure Sockets Layer) Certificate into their Web sites. SSL is used to protect confidential information, such as credit card numbers or passwords, sent between Web users and Web sites. Extended Validation SSL Certificates provide an additional layer of protection through a strictly defined issuance process to ensure that the certificate holding entity is who it claims to be.

“The certificates were developed to combat online scams such as phishing and include unique representations within browsers to demonstrate security to consumers,” explains MRC Executive Director Tom Donlea. For example, Microsoft’s Internet Explorer Version 7 shades the address bar green for Web sites that use EV SSL. The green shading is the only trust indicator that makes an actual change in the browser user interface. All other trust indicators such as site seals are graphics that can be faked.

“It is critical,” Donlea concludes, “for merchants to use EV SSL and other tools to protect themselves and their customers from the latest online hazards.” **TT**

*Julie Ritzer Ross is a contributing writer for Transaction Trends. Reach her at julieros@aol.com.*