



## Fighting Web Fraud

**Security: The Internet has made it easier for crooks to rip our company off. Here's how businesses can protect themselves and their customers**

By Erik Sherman

NEWSWEEK  
June 10, 2002

It was almost too easy. All the young woman had to do was pick a stolen credit-card number and go online.

ACCORDING TO U.S. postal inspectors, she then bought computers and other electronic gear. A measure of the extent: when police swooped down on her New York apartment two years ago, they found \$20,000 worth of gear. And she was identified only because of fraud-detection software. When she made an \$800 purchase at the IKEA furniture and household-goods Web site, a program called eDetective noticed that the shipping address she gave was in a different state from the billing address for her card. This raised a red flag for IKEA fraud manager John Barry. He noticed, too, that the cell-phone number she gave as a contact was in yet a third state. He launched the probe that ended in her arrest for possession of stolen property. She pleaded guilty, apparently to a lesser charge (the case is sealed). But Barry counted it a win for his software. "Anybody who hangs their sign out front to do business on the Web takes a tremendous amount of risk," he says. "The Web gives the thief the edge. We can't see your body language, hear the tone of your voice, see the sweat on your palms."

Fraud has always been a problem for businesses. The Internet has made it easier. According to Visa USA, the rate of online credit-card fraud is three to four times higher than fraud overall. Some industries are peculiarly vulnerable, such as telecommunications. "In the entire telecom industry, the current estimate is that \$15 [billion] to \$20 billion of fraud happens on an annual basis," says Peter Smith, manager of AT&T's global fraud-management center.

But new technologies enable companies to fight back. Given the sheer volume of e-commerce today, software is the only solution. "You may have a suspicion that something is going on, but even if you do see some, it may only be the tip of the iceberg," says Colin Shearer, vice president of data mining at statistical-software company SPSS. "In areas like e-commerce, it's way beyond human capability to check each one of [the transactions]."

One widely used tool is known as rule-based-detection software. Merchants who use it create what is sometimes called a "negative file," stating the criteria each transaction must meet. These might include price limits and matches of the cardholder's billing address to the shipping address for the purchase. The rules might flag an order for an unusually high number of a single item. And they should always maintain current lists of stolen credit-card numbers. The software then screens incoming orders and uses the rules to approve or reject purchases.

A related tool is predictive-statistical-model software. It examines mountains of data from previous transactions to create mathematical descriptions of what a typical fraudulent transaction looks like. It then looks at incoming orders and assigns each one a "risk value" based on its resemblance to the prototypical fraud. AT&T, for example, uses predictive models to sort through its more than 350 million calls a day, identifying a thousand cases of questionable activity. An average of 50 investigators are on duty at any given time examine them to find the 200 cases of actual fraud. "You're literally trying to find the needle in the haystack," says Smith. " [But] if you don't find that needle... you could end up losing tens of millions of dollars within hours." It's worth the effort and expense, though: Smith estimates that AT&T's software blocks "at least" 100 frauds for every one it lets through.

Consumer fraud is not the only threat. In such industries as auto insurance and health insurance, service providers often file fraudulent claims. A body shop, for example, may include in its estimates repairs the car doesn't need. In health care, according to estimates by the Center for Medicare and Medicaid Services, \$100 billion a year is lost in health care to fraud from physicians, hospitals and other agencies that might, for example, use false diagnostic codes in their electronic filings to suggest costlier procedures than were actually done. Detection software can be "tuned" to flag frauds characteristic of a particular industry. "Ninety-six percent of the estimates we review are changed, and the average percent or reduction is anywhere from 11 to 13

percent,” says Eric Seidel, president and CEO of eAutoclaims Inc., whose software lets auto-insurance firms track claims and repair estimates.

Outside help is available. “It’s valuable to have a trusted network outside your company, because that’s where the expertise will be,” says David Fisher, manager of the Verizon Communications fraud-prevention center. Few companies can afford expertise in fraud prevention on the scale of AT&T, so turning elsewhere makes sense. For example, Experian, one of the three big credit-reporting companies in the United States, has developed a cross-industry fraud database. Member companies can check credit applications against problems reported by other members. One of the clients recently ran a week of tests, checking credit applications against the database. “That client had a 2 percent hit rate on the national fraud database,” says vice president of fraud solutions Lyn Porter. “We identified around \$50,000 in savings a day.”

Of course, all the software in the world will be ineffective if the enemy is within. A national retail chain found that its Dallas store suddenly went bankrupt after hiring a new manager. He was diverting sales revenues to himself through an elaborate combination of false invoices and doctored credit-card charges. His inside knowledge helped him sidestep the company’s detection software. “He got away with it for 18 months,” says John Wiechman, president of TLSI Inc., the computer-forensics firm hired to find the evidence. “The company was being run, but it wasn’t being watched real close. [Corporate management] walked into the Dallas warehouse and it was empty.” Even the best systems won’t work for people asleep at the on-off switch.