



Thrust and Parry

By Katie Deatsch

October 31, 2008

<http://www.internetretailer.com/article.asp?id=28308>

How crooks use smooth talk and high tech to evade e-retailers' fraud-detection systems

Web merchants know thieves like to have orders delivered overnight so they only have to watch the delivery address for a short time before making off with their loot. That's why the fraud systems online retailers use often flag a request for overnight delivery as a warning sign of fraud.

The problem is that the thieves have figured that out, and have come up with ingenious ways to avoid tripping those fraud alerts, says Bryan Whitney, contact center director at multi-channel retailer Urban Outfitters Inc. For instance, the thief might request standard shipping when placing the order, then call customer service a day later complaining that the retailer processed the order incorrectly and that he needs the package tomorrow. If the agent is not hip to the trick, the thief gets the order delivered overnight without setting off a fraud alert.

Or, knowing that retailers will look more closely at an order when the shipping address is not the same as the credit card's billing address, some crooks will enter the card's billing address when placing the order on a web site, then call the carrier to have the destination changed, Whitney says.

"The most interesting thing to me is the social engineering aspect," Whitney says. "They really look for ways to circumvent our fraud controls."

It's part of the never-ending battle between thief and retailer. Both sides are employing high technology and social skills in novel ways to gain an edge. Retailers have to keep up to keep from being taken.

"Fraud is evolving," says Allen Weinberg, a managing partner at Glenbrook Partners payments consulting firm. "Criminals adapt. As you plug one hole another one arises."

Educated criminals

Fraud is also increasing. In 2007, 1.3% of online sales later turned out to be fraudulent, up from 1.1% in 2006, according to payment security specialist CyberSource Corp.

Fraud is especially a concern for online retailers who sell high-ticket goods, such as The Watchery.com, whose average sale is \$2,000.

“I just had a fraudulent order today that came from a university in Pennsylvania,” says Joseph Levy, founder and general manager of TheWatchery.com “Here’s a kid that’s probably going to school for computer systems and in his spare time using what he’s learning to place a \$20,000 order with a stolen card.”

The retailer was seeing many fraudulent attempts to place orders, the majority of them for merchandise worth \$7,000 or more, when it decided it was time to invest in more sophisticated antifraud technology. The e-retailer deployed a fraud-detection system from Accertify Inc., a company launched last year by a team of executives who developed the fraud-prevention program for travel web site Orbitz LLC.

Levy likes the Accertify system because it gives him the flexibility to decide what is risky, instead of the system automatically assigning risk when, for instance, the ship-to address is not the same as a card’s billing address. Many of TheWatchery.com’s legitimate customers buy gifts for their spouses, and send them to their work addresses so as not to spoil the surprise.

“The rules that apply for most retailers don’t apply for me and my customers,” Levy says.

The Accertify system analyzes several data points for each order, including price and other parameters Levy prefers not to mention for fear of tipping off criminals. The system also verifies the card’s billing address with the issuing bank.

Accertify says about 10 online retailers use its system, including TheWatchery.com and Urban Outfitters.

Speak the truth

Other new technologies and services are emerging to fight online fraud.

One new system called Victrio records phone calls customer service representatives place to consumers to check on suspicious transactions, and then cross-checks the voice of the consumer against an audio file of the voices of known criminals. The system was recently put to the test to distinguish five crooks’ voices out of a batch of 25 for an online luxury retailer. It scored 100%, says Tony Rajakumar, founder and CEO of Victrio and a former engineer at a speech recognition company.

Victrio is still building its database of audio files, which Rajakumar says will increase as more merchants sign on. “Most crimes come from career fraudsters,” he says. “Merchants aren’t just going to be hit by someone once, but 100 times. If they can put their voice in a database, it will help everyone.”

Another vendor, Ethoca Ltd., touts a fraud-prevention community that businesses, including e-retailers, can join for a fee. Members contribute customer information and can see data from others in the community.

Businesses not only share information on problem customers—such as those who commit fraud or habitually return items—but also about good customers. That helps participating retailers identify transactions that are likely to be legitimate, as well as those that are suspicious.

About 50 businesses have joined the network, which launched in 2005, including e-retailer TigerDirect.com, a subsidiary of Systemax Inc. Subscriptions to Ethoca range in price from \$500 to \$25,000 a month depending on size and usage.

Other services like one from Quova Inc. use geolocation technology to see where a visitor is coming from. The system can help e-retailers spot IP addresses associated with fraud or flag suspicious orders, such as a visitor from Romania attempting to make a purchase with a card tied to an address in Iowa.

Back to basics

While third-party providers are eager to offer services for a fee, Eric Archuleta, CEO of online music instrument retailer Musician's Hut, has decided to fight fraud on his own. In-house business practices can go a long way in thwarting crooks, he says. And, he says, his company can't afford the prices payment security vendors charge.

Requiring a consumer to enter a three- or four-digit code often called the CVV2 or CVC2 code is one basic step that helps, says Archuleta, who has a background in fraud prevention. The code was created by card companies several years ago to reduce fraud on card-not-present transactions.

The short number is not stored on the card's magnetic stripe and so it can't be acquired by skimming, a technique crooks use to capture card data at checkout counters or at ATMs. Therefore entering the code is meant to prove the consumer has the card in hand—and not just a number that can be obtained by swiping a card through an inexpensive magnetic stripe reader.

Some merchants have expressed concern that asking customers to complete another step during checkout could lead to cart abandonment, but Archuleta says that's not his experience. Today, about 40% to 50% of card-not-present merchants capture the security code, estimates payment consultant Steve Mott of the firm BetterBuyDesign.

Musician's Hut also cross-checks the billing address of the credit card with the address on file at the issuing bank. "We will only ship on a full match," he says.

And, the retailer treats international orders with extra caution. "Banks overseas don't go through the same verification procedures as those in the U.S.," says Archuleta.

Indeed, the rate of fraud associated with international orders was more than two-and-a-half times as high as on domestic orders for U.S. and Canadian e-retailers last year, according to CyberSource.

And so, Musician's Hut requires international customers provide copies of the front and back of two forms of government-issued ID and their signature. "If they go to that much trouble, they are likely not going to scam us," Archuleta says.

While Archuleta says it takes time to manually review suspicious orders, and place follow-up calls, he notes an added bonus—the opportunity to build a relationship with the customer.

"There's a big difference between a conversation that starts with 'Hi, we'd like to know why you're stealing from us,' and 'Hi, we'd like to talk with you about your order,'" Archuleta says. "When we're on the phone validating with someone we try to make them feel as comfortable as possible. Any contact with a customer can be positive contact."

But for the purposes of preventing fraud, savvy retailers should ask some questions that a thief might find hard to answer, says Ori Eisen, founder and chief innovation officer at 41st Parameter, a company that specializes in detecting and preventing online fraud. That could include a question such as, What are your nearest cross streets? "If the person lives there, that's something he should easily know," Eisen says. "You'll know right away if he starts to fumble."

Counterattack

For every safeguard retailers deploy, crooks probe for ways to defeat it.

"We had a compromised card from Miami, and the fraudster had the cardholder's Social Security number," says Levy. Having such personal information can make it easier for a thief to call the card issuer and change the billing address to match a shipping address where he can safely receive merchandise.

And crooks are going after systems set up by major card networks specifically to address online fraud, Verified by Visa and MasterCard SecureCode. In both systems, a cardholder who registers chooses a password to enter when making an online transaction, adding another layer of security. Levy says he encountered one crook who had nabbed a consumer's Verified By Visa code, enabling him to thwart the security system.

Where do the crooks get such confidential data? Levy points to phishing attacks, fake e-mails disguised as messages from a bank or financial institution in an attempt to get consumers to reveal personal data. They are especially effective in fooling older consumers, Levy says

But, with many consumers now educated about standard phishing attacks, crooks have learned to personalize their e-mails to make them seem more authentic, a technique called spear phishing that is aimed at defrauding wealthy individuals, says Joey Peloquin, a senior security consultant in the software division of technology provider Hewlett-Packard Co.

A con artist may call an executive's secretary seeking to pry out some personal information, or scour Securities and Exchange Commission filings of the target's company.

“It’s evolved into a highly effective tactic this year and last year,” Peloquin says. “They will find out, Joey has an account with Fidelity and does his banking with Washington Mutual. They will even see what membership organizations a CEO belongs to—that he owns a Porsche and that he is a member of a Porsche organization.” The crooks then use that information to try to extract financial data from the target with personalized e-mails.

Dressing up

Beyond spotting loopholes, scammers also are discovering ways to look more legit.

Crooks have for years used IP spoofing, in which a criminal in a country with a high fraud rate, such as Nigeria, disguises the location of his device so that it appears to the online retailer that the visitor is coming from a safer area.

That has more recently been extended to make use of Internet-based phone systems. Crooks use Voice Over Internet Protocol systems to obtain phone numbers with area codes that match a stolen card’s billing address, says Mike Long, vice president and chief product strategist at Accertify. VoIP systems often let users choose their own numbers, Long says.

And the criminal element has always been among the leaders in social networking, with underground hacking web sites swimming with tips about the easiest retailers to con. “They will say that such and such merchant doesn’t use address verification or doesn’t capture the CVV code,” Long says.

With word of vulnerabilities spreading at Internet speed, online retailers can ill afford to become the talk of the town in Hackersville.