Address-form glitch proves an easy scam

Credit-card thieves find sneaky way to beat fraud checks

By Bob Sullivan
Technology correspondent
MSNBC
Updated: 1:52 p.m. ET Oct. 22, 2004

It's a harmless-looking part of every a Web site retailer's checkout page. The form filled out by customers ordering products almost always has a second line — sometimes it's used for apartment numbers or other information; it's usually left blank. But that innocuous-looking second line could become a big headache for Internet merchants soon, says one fraud expert. Credit card criminals have figured out a simple way to use that second line to foil the most basic anti-fraud measures online merchants use.

Already, five major Web merchants — with sales of $75 million or more each year — have been hit by the hack, says Julie Ferguson, co-chair of the Merchant Risk Council.

"All of the sudden this has risen above the noise (of other scams). That's a good indicator this could be a big deal during Christmas," Ferguson, also vice president of anti-fraud service ClearCommerce Corp, said. The firm planned to issue a warning to merchants this week about the technique.

The hack — and it can only loosely be called a hack — involves tricking the rather archaic address verification system (AVS) used by most merchants, often their first line of defense against fraudsters.

When a consumer gives a Web site a credit card, the site asks the issuing bank — usually through a third-party service — if the account number is valid, and if there is enough credit left in the card's balance. Usually, firms also perform an address verification for an additional charge of a few pennies. That is supposed to ensure the address supplied by the buyer is the same as the address on record for the credit card account at the bank. In the past, criminals have used the "ship to a different address" form to get their stolen items shipped to an alternate location, but long ago merchants became wise to that ploy and often designate orders where the shipping and billing address don't match to get extra scrutiny.

The new, "second-line scam," allows criminals to get past the shipping-billing discrepancy issue. They can use a substitute address in the billing area field, and at the same time, trick the merchant into thinking the correct billing address has been entered.

Designed long ago, most address verification systems only check numerical values at the beginning of the address and zip code fields in the billing

address form. Letters, such as street names and cities, are ignored. That means if the legitimate address is 123 Elmwood Street, and a criminal enters "123 XXTRTWW," the fraud software will return a “yes” value, indicating the address is valid.

Criminals then supply the street and town where they really want the goods delivered in the second line. So a scam address could read:

John Q. Public
123 XXTRTWW
99 First Street
Hackertown, NY 10000

Such an address would raise immediate suspicion with orders that are visually inspected by merchants, but that's rare, Ferguson said.

"Merchants don't manually review very many orders. Most merchants manually review about 10 percent," she said.

The address above might still fail the address test on the zip code field, but merchants often chose to ship a product if the only error in the order is an erroneous zip code, Ferguson said. Or, the hacker may enter the zip code attached to the credit card but the city where the stolen merchandise is to be delivered, and often, the delivery firms will correct the erroneous zip code and deliver the product.

In a more sophisticated form of the attack, criminals trying not to raise suspicion are sure to write valid-looking street addresses that aren't actually in the destination town, to ensure delivery to the second line address.

"But most of the time we are seeing goobly-gook," Ferguson said.

She had seen a few instances of the scam during the past nine months, but received word from five different merchants in the past two weeks asking about the suspicious orders using this ploy.

"They were calling saying, 'What's this?'" she said.

Ferguson predicted the trick would spread quickly, but other merchants indicated they hadn't seen the issue yet. Mike Fisher, who handles dozens of merchant accounts at his firm Merchant Mechanics, said he hadn't seen any second-line fraud orders.

"I have not had experience with that with any of my merchants," he said. "We see lots of flavors of new tricks. You would think any savvy merchant would identify the order as suspicious with garbled characters in the first line. It seems it would be easy to spot."

Dan Clements, who operates merchant advocacy service CardCops.com, also said he hadn't seen the scam yet.

"I don't think it's a big deal," Clements said. But he added that address verification is a easy target. "It is pretty archaic."

While AVS is the most basic form of fraud control, most merchants include some additional fraud protection. Many now require additional numbers called "CVV2" that are found on the back of a credit card. Requesting those numbers is supposed to prove the person ordering the merchandise is actually holding the card. But credit card thieves have caught on to that method, and often come equipped with CVV2 information as well.

Several firms offer additional automated fraud screening software that detects odd ordering patterns, such as multiple orders for expensive merchandise from the same computer attached to the Internet.

But many firms rely on address verification as their main line of defense, and it isn't reliable, Ferguson says.

"The biggest thing is to educate the review team (at Web sites)," she said. "You can look and see if you getting a lot of orders with second address line completed."

Bob Sullivan is author of Your Evil Twin: Behind the Identity Theft Epidemic*.*

10 ways to protect your identity

1. Burn or shred, with a cross shredder, any mail or financial papers with your personal information on it. Never recycle them.

2. Call 1-888-5optout and ask to stop credit card companies from sending pre-approved credit card applications to your house. They are ticking identity theft time bombs.

3. Ask your credit card firm to cease delivery of "convenience checks." They, too, are ticking time bombs.

4. Beginning in December, you're entitled to one free credit report each year. Get it as soon as possible and review it carefully.

5. Order a credit report a month or more before you make a big purchase or apply for credit, to be sure there are no surprises in your history.

6. Hassle companies that ask for personal information, such as your phone number at a checkout line. The harder we make it on companies, the less they will be inclined to continue the practice.

7. It's impossible to tell what's real and what's fake online. Just delete any e-mail that asks for personal information.

8. Just hang up on telemarketers, particularly ones who seem to be fishing for personal information, like your birthday.

9. Limit the number of credit cards you hold, and religiously inspect your financial statements each month. Consumer rights quickly fade over time; the sooner you discover an identity theft incident, the better.

10. Most of the time, you can't prevent an ID theft incident from occurring, because two-thirds of the time, some company that leaked the data is to blame. So be prepared, and be organized. Save paper bank records for a year, at least. You'll need them to prove your account balance in the event of a ID theft incident.