Caller ID spoofing scams aim for bank accounts

March 19 2012, By Byron Acohido

That call you received on your mobile phone might not be from the company that popped up on your Caller ID.

Cyberthieves are stepping up phone-calling scams that pilfer the accounts of consumers who bank online. And many such calls are linked to Caller ID spoofing, which causes the recipient's phone to display a Caller ID number that appears to originate from a trusted party.

In the second half of 2011, Pindrop Security detected more than 1 million fraudulent calls, including 189,439 in December, a 52 percent surge from July, according to a first-of-its-kind report released Thursday.

"Mobile is a growth area," says Stan Stahl, president of the Los Angeles chapter of the Information Systems Security Association (ISSA), which works with financial institutions to stem online banking fraud.

Spoofers often lure a cellphone user into divulging account information via an automated call or text message that appears to come from the user's bank. Next, the crooks call the bank, spoofing the victim's phone number and correctly answering security questions to trick the bank employee into transferring cash or issuing credit cards for mailing addresses under the scammer's control.

Dell SecureWorks estimates small and midsize businesses in the U.S. and Europe lose as much $1 billion a year from online banking accounts.

The financial services industry often does not reimburse such losses. "We'd expect business owners to be a bit more savvy and have more resources at their fingertips," says Carol Kaplan, spokeswoman for the American Bankers Association. "That doesn't mean we're not seriously concerned about the problems small businesses are having, and there continues to be huge gobs of investment into shoring up security."

Results of an ABA survey of 95 financial institutions, released exclusively to USA Today, show the number of commercial account takeovers by cybercrooks rose 260 percent in 2011 vs. 2009. However, the average loss per victimized company decreased 92 percent during the same period.

"Financial institutions are becoming more effective at stopping illicit transactions from being executed," says Doug Johnson, the ABA's vice president of risk management policy.

Consumers are getting hit, too, but if they report thefts promptly, the banks typically bear the loss. Losses from consumer accounts probably exceed "$1 billion a year," estimates SecureWorks' Dale Gonzalez.

Names, phone numbers and e-mail addresses can be purchased inexpensively from hackers who specialize in cracking into databases, such as the gang that swiped 24 million customer records from online shoe retailer Zappos earlier this year.

In the last six months of 2011, bogus calls were placed in connection with scams directed at 30 of the 50 largest financial institutions in the U.S., Pindrop CEO Vijay Balasubramaniyan says. "We are continuing to see this rising trend," he says. "There appears to be a network effect as word of successful scams gets relayed to other fraudsters."

ISSA's Stahl says tech companies and banks need to do more to stem the

tide of attacks. Part of the solution: being more transparent to small businesses and consumers about the risks of online banking.

"Online bank fraud is at epidemic levels. There's no question about that," Stahl says. "Right now there is inadequate security against the many kinds of attacks that lead to online banking fraud, and that's only going to get worse."