



ID THEFT: THWARTED ONLINE, FRAUD GOES LOW-TECH AGAIN

U.S. Banker
Saturday, March 1, 2008

By Glen Fest

The payoff from reducing identity-theft crimes through electronic channels has had some surprising twists. A new study from Javelin Strategy & Research found a continuing overall decline in fraud numbers and victims in the U.S., which is no doubt due to multifactor authentication and other fraud-fighting tools at the disposal of online banking customers. But the research found a significant disturbing new trend: More criminal enterprises are shifting toward off-fashioned "vishing" methods and other inexpensive alternatives to catching unwitting consumers off guard.

Javelin's report, which reported the third consecutive year of declining ID-theft-related fraud losses, jibes with a new Federal Trade Commission ID-theft analysis that shows reports similar figures, even though ID theft remains, at 32 percent, the third most prevalent fraud complaint.

Phone and mail-fraud schemes are skyrocketing, as crooks migrate back to traditional offline scams. Vishing — in which fraudsters convince consumers in phone calls that they are bank representatives needing specific personal or account details — in particular, is flourishing. Such offline schemes grew to 40 percent of all fraud incidents in 2007, compared to only three percent in 2006. "Fraud is very much multi-channel, both high-tech and low-tech," says James Van Dyke, president of Javelin Research.

Overall, fraud losses declined 12 percent in 2007 to \$45 billion over the previous year, according to Javelin. Meanwhile, the number of victims hit 8.1 million people in 2007, a slight decline from 8.4 million in 2006, but a significant decrease from the 10.4 million affected in 2003. For the first time, Javelin also tracked regional ID-theft trends that found more activity in states with dense metropolitan areas, higher incomes and more commerce. California and Illinois, for example, are among five states that were "well above" the national average, it said.

While the ID-fraud incident rate shrunk to just 3.58 percent of the U.S. population in 2007, the per-incident cost to consumers jumped 25 percent to \$691 per episode. "We have two opposite trends going on," says Van Dyke.

Another persistent trends seen by investigators is the rise of family- or friend-related ID theft. Many victims remain reluctant to prosecute suspects if the thieves are friends or family, and their delay in making that decision may be responsible for the higher per-incident charges, say investigators. "The victim [would like] it both ways: They want losses returned by the bank, but they don't want to see a nephew — John with a drug habit — winding up in jail," says Van Dyke, who says there are indications that this kind of suspect may be part of a growing trend.

If a growing number of consumers are getting taken on the telephone or by people they know at home, anti-fraud software and other techniques would be hard-pressed to stop this activity. No multi-factor authentication, biometric or password-protected Website lockdown can be built to prevent the criminal actions of a shady acquaintance welcomed into a consumer's home.

Steve Coggeshall, chief technology officer of ID Analytics, points out that synthetic ID fraud — the wholesale creation of fake names to defraud banks — also continues unabated. "For fraudsters, it's like

squeezing jello," he says. "They look for the simplest methods to commit their crime. Synthetic identity fraud tends to be attractive, but the victim in that case is the business."

New-account fraud activity may be changing form, particularly as know-your-customer regulations take hold at banks. New wireless-phone accounts have increased to 32 percent from 19 percent of new fraudulent accounts, and are now "exceeding fraudulent new credit cards, loans, checking or savings accounts" in the criminal use of another person's information, according to the report.

Multifactor authentication and credit file monitoring remain the strongest vehicles for consumer self-directed protection, although Van Dyke believes banks should do a better job overall of giving customers real-time, credit-report alerts.

(c) 2008 U.S. Banker and SourceMedia, Inc. All Rights Reserved.