



## ID Theft

### THWARTED ON-LINE, CRIME LOOKS TO PAST

Bank Technology News | Saturday, March 1, 2008  
By Glen Fest

The payoff from reducing identity theft crimes through electronic channels is not what we've expected. In a new identity theft report survey, Javelin Strategy & Research found a continuing overall decline in fraud numbers and victims—no doubt due to multi-factor authentication and other fraud-fighting tools at online banking customers' disposal. But the research finds a rapidly evolving criminal enterprise shift toward "vishing" and other hands-on, lo-fi alternatives to catching consumers off-guard.

Javelin's report, which found a third consecutive year of declining ID theft-related fraud losses, largely jibes with a recent FTC identity theft fraud report in which both the number of victims and incident rates have shrunk. But phone and mail fraud schemes are skyrocketing as crooks migrate to more traditional offline scams. In particular is vishing, in which fraudsters convince consumers they are bank representatives that need personal or account details over the phone.

Such offline schemes have elevated from being just three percent of ID theft cases in 2006 to 40 percent of all cases last year. "Fraud is very much multi-channel, both high tech and low tech," says James Van Dyke, president of Javelin Research.

Overall, fraud losses declined \$6 billion (or 12 percent) to \$45 billion. (The FTC reported only \$15 billion in fraud losses, but the government numbers track actual reported cases whereas Javelin extrapolates national numbers based on its research.)

Javelin estimates the number of 2007 victims is 8.1 million people, a slight decline from last year's 8.4 million, but a significant decrease from 2003's 10.4 million. Still, ID theft remains the most prevalent fraud complaint to the FTC (32 percent).

For the first time, Javelin also tracked regional ID theft trends that generally found more activity in states with dense metropolitan areas, higher incomes and more commerce. California and Illinois are among five states "well above" the national average.

The incident rate has shrunk to 3.58 percent of the U.S. population. Unfortunately for consumers, that decline is not reflected in the per-incident expenses victims had to pay for stolen identities. That's gone up 25 percent to \$691 per episode, which may sound a little fishy (not phishy) since the average amount criminals steal is going down. "We have two opposite trends going on," says Van Dyke, which might be explained with the rise of fraud-by-proximity.

He says investigators see a trend where some ID fraud victims are more reluctant to prosecute since the thief is a suspected relative, and end up eating the fraudulent charges. "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.

Consumers are getting taken on the telephone or by their own friends and relatives to an extent that might be greater than previous reports from Javelin, the FTC or other research organizations have been able to tap. No multi-factor authentication, bio-password enabled lockdowns on an online banking site are built to stop a shady acquaintance who was welcomed into a consumer's home.

The friends-'n-family quotient is just one example of where hidden fraud may be quietly flourishing. Steve Coggeshall, chief technology officer of ID Analytics, points out that synthetic identity fraud – the wholesale creation of fake names to defraud institutions—continues unabated. “For fraudsters, it’s like squeezing jello – they look for simplest methods to commit their crime. The synthetic identity fraud tends to be attractive,” says Coggeshall. “But the victim in that case is the business.”

New-account fraud activity may be changing forms as know-your-customer regulations at financial institutions take hold. New wireless phone accounts have increased from 19 to 32 percent of new fraudulent accounts, and are now “exceeding fraudulent new credit cards, loans, checking or savings accounts” in the fraudulent 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 Javelin’s Van Dyke thinks banks can do a better job overall in giving customers real-time, credit-report alerts (instead of insisting it remain a marginal profit center).

Some industry observers have expressed worries that more interactive and social networking aspects of the Web may expose consumers further, but Van Dyke thinks it may have the effect of improving vigilance.