



Access the IAM analyst report >



COMPUTERWORLD Security

 Print Article  Close Window

ID theft forecast: Gloomy today, worse tomorrow

Gregg Keizer

March 07, 2007 (Computerworld) Virtually every trend line for identity theft is bad news, a research analyst said today as she released a survey showing that 15 million Americans were victimized during a recent 12-month span.

For the year-long period that ended last August, 15 million people were burned by some kind of fraud related to identity theft, said Avivah Litan, a Gartner Inc. analyst. That number is 50% higher than 2003 data released by the Federal Trade Commission.

Other figures from Litan's study were equally downbeat. The average identity theft fraud loss more than doubled in 2006 to \$3,257 from \$1,408 the year before, while the percentage of recovered funds dropped to 61% in 2006 from 87% in 2005. The average loss on new-account fraud -- where criminals use the data they've stolen to open new credit card or bank accounts -- was \$5,962 in 2006, a jump of 223% over 2005's \$2,678. And unauthorized charges to credit cards leaped nearly fourfold, to an average last year of \$2,550. Unauthorized charges in 2005 averaged just \$734.

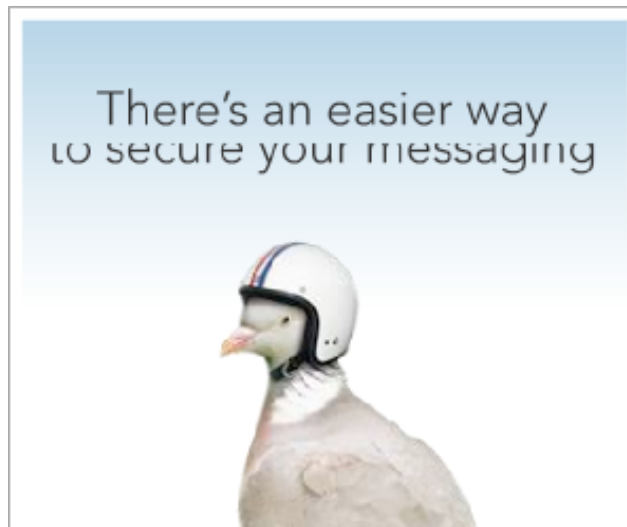
"What's useful here are the trends; the numbers can never be exact," Litan said. "The only good news, and it's not much, is for banks. They're less on the hook than before. They're not getting attacked directly as much now."

That's because criminals are increasingly turning to unconventional identity theft ploys rather than tackling the banks themselves. Financial institutions have, at least in the cases of large banks, fortified their data. "Hackers are exploiting Internet auctions, money transfers like Western Union and PayPal, the ability to impersonate lottery and sweepstake contests, and other types of imaginative scams," said Litan. "They're going after the weakest links, the consumers using social engineering tactics, and the U.S.'s payment systems at retail and businesses."

Of those surveyed who knew or suspected the causes of the identity theft, data breaches led the charge with 15%. "Banks eat the fraud there," at least for now, said Litan. A [Massachusetts state lawmaker](#), however, has proposed a bill that would hold retailers financially responsible for breaches.

Litan scoffed at the idea. "The retailers are already paying for fraud" in the form of higher interchange charges, she said. "The banks are already collecting this. What are they doing with it?"

In fact, Litan didn't hold out a lot of hope for change, at least in the short run. "Identity thieves have gotten



more clever," she said. "The only way this will be solved is if the data is rendered useless if it's stolen. Then it won't matter if they steal it." She offered up examples of how that might be done, including more sophisticated authentication on debit cards and payment processors relying on identity scoring systems that were able to spot thieves using indicators like physical location.

"But I really think that it will take an extreme attack of some kind and broad disruption before things change," Litan said. When asked what form such an attack might take, she put forward a pair of scenarios.

"We know [that criminals and cyberterrorists] are collecting tens of millions of records, maybe as many as 100 million. They might just publish them all on the Internet. Or a massive attack on banks, a massive number of bank account takeovers all at once," she said. "A simultaneous attack like that would slow commerce down. It would be a kind of financial 9/11."