



ID Theft Is Exploding In The U.S.

The number of victims and the amount stolen are both ballooning, according to a new study.

By Sharon Gaudin, [InformationWeek](#)

March 7, 2007

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=197800774>

Identity theft is exploding in the U.S., with 15 million Americans victimized in just a 12-month period, according to a new study.

The amount of money that is being stolen from them is on the rise, as well, more than doubling between 2005 and 2006, Gartner analysts report in a study. And more of what they're losing is staying lost. The report also shows that people managed to recover 87% of what was stolen from them back in 2005, but in 2006 that number dropped to 61%.

"Hackers are exploiting Internet auctions, non-regulated money transmittal systems, the ability to impersonate lottery and sweepstake contests, and other types of imaginative scams," said Avivah Litan, a VP at Gartner, in a written statement. "The thieves have also discovered the weakest links in the U.S. payments systems. Typically the weak links are found among the five or more million businesses that accept electronic payments from consumers, and the consumers themselves."

Gartner's survey of 5,000 online U.S. adults in August 2006 showed that the rate of identity theft has jumped by 50% since 2003 when the Federal Trade Commission reported that 9.9 million Americans had been victimized. The average loss was \$3,257 in 2006, up from \$1,408 in 2005.

Unauthorized charges to credit cards rose nearly fourfold from an average of \$734 in 2005 to \$2,550 in 2006, Gartner reports. These numbers go along with a trend cited by various U.S. credit card issuers that reported large increases in counterfeit card fraud last year. Similarly, there were large increases in checking account transfer fraud and "other" non-categorized types of fraud, such as scams exploiting eBay, PayPal and phone companies.

"Oftentimes, consumers have no idea how criminals hijack their accounts and/or identities," Litan said. "They also typically have no clue if one or more of their personal attributes, such as their Social Security number, is used to piece together a new fictitious identity in a phenomena typically referred to as synthetic identity fraud."

Gartner contends that fraud can be largely prevented by using identity verification and scoring services, which are independent services used to calculate personal credit scores.

"Enterprises who store credit card, debit/ATM card and bank account data should expect electronic data breaches and/or hacks, and migrate away from that practice while protecting their systems accordingly until they are able to do so," Litan said. "Rule-makers debating identity-theft legislation should consider comprehensive financial protection for consumers who lose money to fraud that goes beyond disparate regulations in place today. Service providers should pay for this protection when data or accounts under their custody are breached."

Identity theft has been in the news a lot in recent months with government agencies and businesses suffering network breaches or losing laptops containing critical information. Last month, the Department of Veterans Affairs announced that a [hard drive that went missing](#) in January actually may contain sensitive information on about 535,000 veterans, along with 1.3 million doctors. And a laptop stolen from a secure office in the Seton Family of Hospitals in Texas is putting at risk

[identifying information on 7,800 patients](#) without health insurance. In February, hospital administrators reported that a security camera captured [video](#) of the thief carrying out a laptop, which contained identifying personal information, such as Social Security numbers, dates of birth, and insurance program numbers.



Copyright © 2006 [CMP Media LLC](#)