



SmallcapInsights.com



ID Theft: A Fast-Growing Global Problem

ARTHUR GOLDGABER | MARKET ANALYST

Identity Theft: A Fast-Growing Global Problem

The Internet has made conducting numerous daily activities such as online banking and communicating with friends much easier. Unfortunately, global computer networks have also made it easier and much faster for thieves to steal people's social security numbers, credit card numbers and to use the data to perpetuate a wide variety of fraud.

Identity theft, also known as "identity fraud" is generally defined as the fraudulent use of someone else's information without permission to open credit cards or bank accounts, write bad checks or take out loans and/or to sell the information. This means that a victim of identity theft is left with the consequences of his or her imposter's actions, whether he or she is aware of it or not. These crimes can threaten everything from a person's finances and personal reputation, to their livelihood and physical health. The consequences of the theft can go on for years as victims can be left with countless charges, years of bad credit and endless aggravation.

As a whole, consumer fraud victims are incurring \$4.8 billion in out-of-pocket costs due to identity fraud. These out-of-pocket losses comprise unreimbursed losses, lost wages due to the time required for fraud resolution and possible legal fees associated with investigation and prosecution.¹

Research by the Identify Theft Resource Center estimated the average out-of-pocket expenditures for victims of identity theft. In the center's report, "The Aftermath 2007", respondents in 2007 spent an average of \$550.39 in out-of-pocket expenses for damage done to an existing account. In reference to new accounts, respondents spent an average of \$1,865.27 compared to \$1,342 in 2006. Victims reported spending an average of 116 hours repairing the damage done by identity theft to an existing account used or taken over by the thief. Victims reported a number of additional problems including: increases in insurance rates, current credit card interest rates and criminal records not being cleared.²

A report prepared by François Paget, a senior virus research engineer for McAfee, explains why theft of personal data on the online world is much more of a threat than in the physical world. In the physical world, a person's identity is concrete and is supported by legal documents. While in the online world, a person's identity is less tangible. Some digital data, such as passwords, account names, screen names and logins, may not be considered elements of a person's legal identity. Yet such data can be "identifying" and provide access to other data.³

Even extremely sophisticated people such as Federal Reserve Chairman Ben Bernanke can be victims of scams. On August 7, 2008, Bernanke's wife, Anna, had her purse stolen off the back of

her chair in a Southeast Washington, D.C.-area Starbucks. In a statement provided by a Federal Reserve spokesperson, Bernanke stated, “Our family was but one of 500 separate instances traced to one crime ring. I am grateful for the law enforcement officers who patiently and diligently work to solve and prevent these financial crimes.”⁴

Concerns about identity theft have helped create a billion-dollar market for credit-monitoring services, identity theft insurance and other products.

Unfortunately, those concerns are justified. The FBI estimates that U.S. businesses lost \$67.2 billion per year to computer crime, according to an article in *USA Today*. The article describes online criminal forums where identities are bought and sold, with prices ranging from \$500 for a credit card number with a personal identification number (PIN) code, down to \$7 for a credit card number with just the expiration date.⁵ The latest numbers from the Federal Trade Commission (FTC) on identity theft are from 2003. The FTC has estimated that, during 2003, almost 10 million Americans discovered they were the victims of identity theft, with a total cost to businesses and consumers of over \$50 billion.⁶

The number of fraud incidents grew 22% in 2008, according to Javelin Strategy & Research’s 2009 Identity Fraud Survey Report. Some 10 million U.S. residents were victimized in 2008, up from 8.1 million in 2007, Javelin reported.⁷ In addition, the Federal Trade Commission received 313,982 identity-theft complaints, up from 215,000 in 2003. The upward trend has been amplified by the increasing sophistication of global identity theft rings, the rising market for secondary financial information and the availability of fraud toolkits online.⁸

According to another report, The Kroll Global Fraud report, the financial services industry has been hit the hardest by fraud with companies losing an average of \$15.2 million each over the past three years. The Kroll Global Fraud report found fraudulent activity in the financial services industry was up by 9% from last year’s total loss of \$12.9 million despite fraud activity across sectors remaining largely steady in 2009.⁹

Thieves employ both sophisticated scams through computer networks and simpler methods. Despite the prevalence of online fraud, low-tech attack methods—stolen wallets, checks, credit cards or mail—still represent the most common way that personal information is obtained. Forty-three percent of fraud incidents where the method of compromise was known involved such methods.¹⁰

It may be for this reason that women were 26% more likely to be the victims of identity theft than men in 2008. According to Javelin’s report, women make more purchases in stores, where low-tech attack methods can be applied. Nevertheless, one measure of that sophistication is the speed at which identity thieves strike. In 71% of reported incidents, the report says, the fraud began less than a week following the theft of the data. That’s 33% faster than fraud incidents in 2005.¹¹

Fraud arising from online access to information accounted for only 11% of incidents with known methods of compromise. However, only about 35% of fraud victims know how the thieves obtained their private information.¹²

Cyber thieves employ many different techniques to illegally obtain people's sensitive information. More than 5 million U.S. consumers lost money to "phishing" attacks, where people are lured into submitting their personal information through fake web sites and other techniques, in the year ending September 2008, a 40% increase over the number of victims a year earlier, according to Stamford, Conn.-based research firm Gartner Inc.¹³ Cyber thieves have also managed to hack into company's computer networks and steal credit card numbers.

A recent arrest of one identity theft ring revealed that the group was able to steal 40 million credit card numbers from retail chain TJX Cos. The same group was charged by federal authorities of stealing more than 130 million credit and debit cards from the computer network for Heartland Payment Systems, one of the country's largest processors of credit and debit card payments, as well as from several major retailers, such as the 7 Eleven convenience store chain and grocery chain Hannaford Bros. Co. TJX alone has spent more than \$132 million on expenses related to the breaches, including the cost to investigate and contain the intrusion and for lawsuits and other legal claims.¹⁴

Global losses from all forms of Internet scams are estimated at over \$3 billion already, and rising. The problem is that while law enforcement usually stops at the national border, cybercrime operates globally. Cybercrime is hard to track, the perpetrators and the scene of the crime are elusive and international cooperation in preventing cybercrime is hampered by bureaucracy.¹⁵

Global security measures are slowly becoming a priority with national governments and strategies and conventions in combating cybercrime, such as the UN General Assembly resolutions 55/63 and 56/121 on Combating the Criminal Misuse of Information Technologies and the Convention on Cybercrime of the European Council, are taking shape.¹⁶

With these types of threats, consumers are looking for theft protection beyond the normal channels. Credit cards may be safeguarded, but that will not help a consumer if the thieves open new lines of credit. Credit monitoring only alerts a victim after an identity theft has occurred. Neither method will help prevent identity theft, or help in resolving the difficult problems once a thief has his or her hands on personal data.

In addition, consumers who sign up for identity theft protection services that focus on credit report monitoring may still be vulnerable to personal information fraud perpetuated by identity thieves that will not appear on credit reports, according to the FTC's report, "Consumer Fraud and Identity Theft: January-December 2007." Credit card fraud and loan fraud activity will appear on a credit report and alert a victim about a possible identity theft incident, but that type of crime only accounted for 31% of the complaints in the Identity Theft Data Clearinghouse maintained by the FTC and the FBI, according to the latest data. That means that about 69% of identity theft

incidents involved many other types of identity fraud such as phone or utilities fraud, employment-related fraud, bank fraud, government documents or benefits fraud (including filing fraudulent tax forms and other types of identity theft that a victim would not know about unless he or she can monitor thousands of databases that collect this data and obtain notice of the identity breach).¹⁷ That is why future efforts to prevent identity theft will have to focus on every method that thieves can employ to derive benefits from someone else's identity, not just credit card theft.

Sources:

- ¹ Javelin Strategy & Research's 2009 Identity Fraud Survey Report.
- ² Identity Theft Resource Center. "Identity Theft: The Aftermath 2007." http://www.idtheftcenter.org/artman2/publish/m_press/Identity_Theft_The_Aftermath_2007.shtml
- ³ Paget, François. "Identity Theft." McAfee White Paper, January 2007.
- ⁴ "Identity Theft Ring Ensnared Fed Chairman Bernanke." *Techweb*. August 27, 2009.
- ⁵ Acohido, Byron and Swartz, Jon. "Cybercrime Flourishes in Online Hacker Forums." *USA Today*. October 11, 2006.
- ⁶ "Putting an End to Account-Hijacking Identity Theft." <http://www.fdic.gov/consumers/consumer/idtheftstudy/index.html>
- ⁷ Javelin Strategy & Research's 2009 Identity Fraud Survey Report.
- ⁸ Liberman, Gail and Lavine, Alan. "Scams Targeting Consumer Accounts are on the Rise." *Marketwatch.com*. April 28, 2009.
- ⁹ "Financial services hardest hit by fraud, Kroll reports." *Investment Advisor*, October 26, 2009.
- ¹⁰ Ibid.
- ¹¹ "Identity thieves face pay cut." *Techweb*. February 11, 2009.
- ¹² Javelin Strategy & Research's 2009 Identity Fraud Survey Report.
- ¹³ Liberman, Gail and Lavine, Alan. "Scams targeting consumer accounts are on the rise." *Marketwatch.com*. April 28, 2009.
- ¹⁴ Wallack, Todd. "Hacker pleads guilty in data theft." *The Boston Globe*, September 20, 2009.
- ¹⁵ "Staying safe online." *Business & Finance*, September 10, 2009.
- ¹⁶ Ibid.
- ¹⁷ "Consumer Fraud and Identity Theft: January-December 2007." Federal Trade Commission, February 2008, p. 14.

Disclosure Statements:

This white paper by Arthur Goldgaber ("AG"), a contributing Market Analyst for SmallcapInsights.com, is to be used for informational purposes only. AG may be engaged from time to time by clients of SmallcapInsights.com to report on macro-economic and general market conditions. This paper is based on information assumed to be reliable and accurate, but AG does not guarantee or make any representation with regard to its reliability, accuracy or completeness. AG made no attempt to independently verify the reliability, accuracy or completeness of this information utilized in the writing of this paper. Any statements or opinions expressed in this paper are subject to change without notice. AG accepts no liability with regard to any loss arising from any use of this paper. These white papers may vary in cost, but in no event will a paper cost more than \$1,000. AG was paid by ID Watchdog, Inc. (IDWAF) in advance of the publication of this paper.