



What the Numbers Tell Us and What You Can Do About It

Indiana Alumni Magazine, May/June 2006

By Fred H. Cate

In February 2005, ChoicePoint, one of the nation's largest information brokers, announced that criminals had obtained access to its records on more than 160,000 people. The announcement set off an avalanche of similar reports of personal data held by institutions being lost, stolen, or improperly accessed. Bank of America, Lexis-Nexis, HSBC, Polo Ralph Lauren, the University of California Berkeley, Ameritrade, Northwestern University, DSW Shoe Warehouse, Time Warner, and, in the fall of 2005, the IU Kelley School of Business were among the more than 120 institutions that reported breaches involving personal, often sensitive, information about 57 million Americans.

The breaches have prompted considerable concern and numerous stories in the press about the risk that they pose for identity theft. Legislators in 22 states responded by passing new and more stringent laws requiring institutions who suffer breaches to notify individuals and take other steps to guard against the compromised data being used to commit identity theft.

Calls for federal data breach legislation have become so great that action this year appears certain. Even without new law, however, in January the Federal Trade Commission imposed the largest fine in its history — \$15 million — on ChoicePoint for failing to adequately protect consumer data.

Much of the hype over information-security breaches reflects the often-repeated statements that “breaches fuel identity theft” and that identity theft is the “nation’s fastest-growing crime,” affecting one out of every five Americans.



These are indeed sobering claims. The problem is, they are not accurate.

But beware: Identity theft is still a serious problem, and newly emerging threats are likely to greatly exacerbate the danger.

The Size of the Identity Theft Problem

According to a January 2005 study by the research firm Javelin, 9.3 million adults — one in 24 Americans — reported being victims of “identity theft.” The number of victims had actually fallen by 800,000 over the prior 16 months, according to an identical September 2003 study commissioned by the Federal Trade Commission.



Professor Fred H. Cate notes that the most likely threat of identity theft lies in the theft of credit cards and checks. He recommends being wary of scams via telephone, e-mail, and the postal service.

Even these figures appear to overestimate the magnitude of the problem. One reason is the breadth and imprecision of the term “identity theft,” which Congress defined in 1998 to mean the illegal use of another person’s “means of identification.” Using a fake ID to gain entrance to a bar or attempting to use someone else’s airplane ticket or season pass is included as identity theft.

More problematically, the term also includes attempting to use another individual’s credit card. In fact, the FTC reports that two-thirds of identity theft incidents are actually credit-card fraud. As long as there have been credit cards, there has been credit-card fraud.

In the long run, whether or not you include credit-card fraud under the broad term of identity theft, this is good news because Congress long ago limited consumer liability to \$50 for credit-card fraud. Universal industry practice is to waive that charge. As a result, individual victims of credit-card fraud pay none of the loss; the credit-card issuer or the merchant covers all of the cost.

The story about credit-card fraud is also good news because it, too, is on the decline. The total cost of credit-card fraud decreased 10 percent, from \$882 million in 2003 to \$788 million in 2004. In fact, from 1992 to 2004, the Nilson Report, which tracks trends in the financial services industry, found that the cost of credit-card fraud had fallen by more than two-thirds. Fraudulent charges are lower as a percentage of credit-card use in the United States than anywhere else in the world.

According to the 2005 Javelin study, 38 percent of identity-theft victims report that they did not notify anyone of the crime — not the police, not their credit-card company, not a credit bureau. It is hard to believe that many people would discover real financial fraud being committed in their name, but choose to pay for the fraud rather than tell someone about it.

If you remove run-of-the mill credit-card fraud and people who didn’t bother reporting the alleged theft to anyone, the more accurate number of victims of “identity theft” may be closer to 2 million people, or one out of every 112 adult Americans. Identity theft is not the run-away problem that many would have us think. Better yet, it is not on the rise. In fact, preliminary data from a 2006 Javelin study show that the number of victims has fallen by another 400,000 over the past year.

More good news is the fact that most victims of identity theft suffer no financial or physical harm. The most recent data available indicate that 68 percent of victims of identity-based frauds report suffering no economic loss and paying no out-of-pocket expenses.

The Cause of Identity Theft

Moreover, information-security breaches rarely appear to be the cause of identity theft. A new study by ID Analytics, which operates a nationwide fraud-detection network, found that even when the missing information included credit-card numbers or other account-level data, only one out of every 1,020 account holders were likely to be the targets of any attempted fraud. This risk is statistically the same as the average for accounts from which no information had been lost or stolen.

These findings confirm what victims of identity theft have been telling government officials all along: to find the source of most identity theft you have to look closer to home. In the 2005 Javelin survey, for example, for the half of victims of identity-based frauds who reported knowing from where their information had been obtained, the most common source of personal information, by a factor of 2-to-1 over any other category, was “lost or stolen wallet, checkbook, or credit card.”

In fact, 35 percent of identity-theft cases in which the perpetrator was identified involved a “family member or relative,” and 18 percent involved a friend or neighbor. That means that half of all known identity thieves were not strangers. Another 23 percent of identity-theft cases involved a dishonest employee. Taken together, three-fourths of identity-theft cases did not involve any access to third-party data that might be obtained through a security breach.

The security breaches we have heard so much about over the past year appear not to be a significant contributor to identity theft. In fact, many security experts suggest that these breaches are nothing new. The reason we hear so much more about them is because a new California law requires public disclosure. There is no evidence that breaches themselves are on the rise.

Moreover, there is cause for caution about what constitutes a security “breach.” Most state laws apply the term to any missing or illegally accessed information. This includes lost or misplaced disks or backup tapes, stolen laptops and cell phones, hacked data, improperly secured Web sites, data lost or stolen in transit, and misdirected mail.

The California Office of Privacy Protection reports that most of the 2005 breaches it tracked were accidents, rather than the result of deliberate attacks, and many involved lost or misplaced information or equipment, rather than any evidence of stolen information. So breaches, like identity theft, may not be as big a problem, statistically, as some initially thought. This is even better news, because while there is little individuals can do to protect their personal data held by third parties, there are important steps each of us can take to protect against our credit cards or checks being stolen or borrowed by our friends and neighbors (see box above).



The Cost of Identity Theft

Although identity theft is not the runaway epidemic many have claimed, it still poses real risks and can be very problematic. The 2005 Javelin study reported that while two-thirds of victims lost no money, the burden on the remaining third was so great that the average out-of-pocket cost per victim was \$650, and the time spent to resolve the fraud was 28 hours

Identity theft also poses significant risks for businesses. In 2004, U.S. business suffered \$50 billion in losses from identity-based frauds. Similarly, businesses suffer significant financial injury through the loss of consumer and market confidence when an information-security breach occurs, even if no identity theft results. A 2003 study found that firms victimized by an information-security compromise that involved theft of credit-card information suffered a stock market loss of 9.3 percent on the day the incident was announced, increasing to 14.9 percent over three days.

These losses are ultimately passed on to consumers through higher prices, reduced service, and lost jobs.

The Future of Identity Theft

Another cause for concern is mounting evidence that identity theft is evolving and becoming more organized. For example, many recent frauds reflect key similarities — common addresses, phone numbers, targets, and strategies — that cause law enforcement officials to believe they are orchestrated by well organized and well financed perpetrators.

Similarly, we appear to be witnessing an evolution of attack strategies that suggests the involvement of sophisticated fraud rings. As one vulnerability in information security systems is identified and patched, attacks evolve to target other weak spots. As leading companies enhanced their information security, attacks have clearly increased against the information held by less well prepared institutions.

ID Analytics' 2005 study shows that efforts to exploit fraudulently obtained identities — for example, by attempting to open new accounts in those names — end as soon as the theft of those identities is made public. This suggests that fraud rings are carefully monitoring how long they can use a stolen identity.

What You Can Do to Protect Yourself

- Keep track of important documents, including credit cards, drivers licenses, and checks. Documents that you don't use very often, such as passports or replacement checks, should be kept in a secure place.
- Destroy pre-approved credit-card and mortgage offers. A good cross-cut shredder for about \$30 is an excellent investment.
- Check credit-card and bank-account statements regularly. Look for charges or payments — even for small amounts — that you don't recognize, and inquire about them with your bank.
- You are entitled by law to a free credit report annually from each of the three national credit bureaus. Look for accounts, credit lines, or other activity that you do not recognize. Report anything you have questions about to the relevant credit bureau. They are required by law to investigate. (For contact information, see below.)
- Use strong passwords that are not real words and include number and punctuation symbols for all online accounts. Do not reuse the same password for all accounts. Change passwords regularly and don't write them down near your computer.
- Don't click on links embedded in e-mails. If you want to go to a Web site, type in its address in the browser window.
- Don't click on attachments in e-mails from people you do not know.
- If you find evidence that you may have been the victim of identity theft or credit-card fraud, report it promptly both to the companies involved and to your local police or sheriff's office. Get and keep a copy of the police report.
- The Federal Trade Commission provides extensive information for consumers on its Web site: www.consumer.gov/idtheft. You can also report identity theft there or via the FTC's Identity Theft Hotline: (877) 438-4338.
- You can also place a fraud alert on your credit report to make it harder for anyone else to obtain credit in your name. You only have to request the alert to be added by one credit bureau, which will communicate it to others. Below is contact information for the three national credit bureaus:

Equifax
(800) 525-6285
P.O. Box 740242
Atlanta, GA 30374-0241
www.equifax.com

Experian
(888) 397-3742
P.O. Box 9532
Allen, TX 75013
www.experian.com

TransUnion
(800) 680-7289
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834
www.transunion.com

More significantly, we are witnessing the emergence of new and harder-to-detect frauds. "Phishing" is one frightening example. Phishing refers to efforts, usually by e-mail, to impersonate a legitimate business or other institution in an effort to trick an individual into providing personal information.

For example, an e-mail that claims to be from eBay asks customers to verify their account information on what purports to be an eBay Web site. Unbeknownst to eBay or the customer, the log-in information is sent to the phisher, rather than eBay, and the phisher can then use it to capture the customer's account information, including credit-card and bank-account numbers and other personal identifying information.

Phishing attacks can lead not only to financial fraud, but also illegal access to sensitive corporate and government networks and the creation of false identities that can be used to commit other crimes, including terrorist attacks.

Phishing attacks more than tripled during 2005. A December 2005 study from America Online and the National Cyber Security Alliance shows that phishing is remarkably successful. Seven in 10 Internet users say they have been fooled by phishing messages.

The perpetrators of phishing scams are also difficult to track down. Many operate outside of the United States, and the average time a fraudulent site stays active on the Web is less than six days.

In addition, evidence is emerging of a new type of identity fraud: synthetic identity fraud. Rather than making fraudulent use of an existing credit card or bank account, or opening a new fraudulent account in the name of an unsuspecting victim, synthetic identity theft involves creating an entirely new identity. The perpetrator applies for prepaid credit-card, cellular, and similar accounts in the name of the nonexistent individual. This creates a credit report, which is the key to applying for high-limit credit cards and unsecured loans. The perpetrator obtains as much money as he can before disappearing.

Synthetic identity fraud requires good organization and up-front money, but multiplied across thousands of accounts opened in the names of nonexistent people, it can be very lucrative. Moreover, it is hard to detect since the fraudulent activity doesn't show up on anyone's credit-card statement or credit report. In fact, it may not be visible for years, as thieves develop credit records for the new identities they have created.

Synthetic identity fraud poses significant risks for businesses and others that grant credit or provide products and services to the nonexistent, "synthetic"

person. And it can be very dangerous for society more broadly if the frauds perpetrated by the creators of the synthetic identities become widespread or if those identities are used by terrorists to gain access to airplanes, government buildings, or other critical infrastructure.

Solutions

Solutions to identity theft, like the crime itself, are complex and ever-changing. Technology plays an important role, as suggested by the financial industry's success in using computer technologies to detect and prevent most fraudulent charges and bank withdrawals.

Law also plays an essential role in deterring fraud and creating incentives for financial institutions, technology developers, and institutions that hold sensitive personal information to protect consumers.

But the fight against identity theft is an arms race, with technological and legal tools always racing to keep up with, and always lagging behind, constantly changing frauds. As a result, the most important weapons in the fight against identity theft continue to be individual action and cutting-edge research.

There are many steps that individuals — and, often, only individuals — can take to protect themselves. There is nothing that industry or government can do to protect individuals who use weak passwords or share them with friends, who fail to check their credit-card and banking statements for fraudulent transactions, or who do not report evidence of identity theft when they find it.

Research is equally critical to understanding and fighting identity theft today and to identifying and countering new threats before they become widespread in the future. One criticism of many recent identity theft-related laws is that they have ignored available research and focus scarce resources on less likely threats, such as information-security breaches, while ignoring far greater threats, such as the theft of credit cards and checks.

The more government, industry, and individuals know about identity theft, the safer we can be today and tomorrow.

-

Fred H. Cate is a Distinguished Professor at the Indiana University School of Law—Bloomington and director of the IU Center for Applied Cybersecurity Research.

What IU Is Doing to Protect the Public

Indiana University is actively involved in the quest to make consumers' digital information more secure and in the fight against identity theft. The IU Center for Applied Cybersecurity Research helps to coordinate and fund those efforts, which include:

- Research on many aspects of information security, including network security, identity verification, encryption, security in portable computing devices, and phishing and other forms of computer-aided fraud.
 - A wide range of new courses and undergraduate and graduate degrees offered through Informatics, the Kelley School of Business, the School of Law, and the IUPUI schools of Science and Engineering & Technology.
 - Capability in operational cybersecurity: IU was one of the nation's first universities to establish an Information Technology Policy Office and an IT Security Office, whose staff provides national leadership in this field.
 - The Advanced Network Management Laboratory in the Pervasive Technology Labs, which provides expertise in the management and security of advanced high-speed networks, including network engineering and tool development.
 - A variety of efforts to provide practical education in security and trustworthy computing to students in other fields, and to civic groups, professionals, legislators, judges, journalists, and others in the community.
 - The Research and Education Information Sharing and Analysis Center (REN-ISAC), which IU operates in close cooperation with the Department of Homeland Security and other ISACs serving other economic sectors, and which serves as a mechanism for gathering and disseminating information, facilitating communication, and developing best practices about vulnerabilities, threats, intrusions, and anomalies affecting higher education.
 - Leadership roles in professional groups, on National Science Foundation and National Academy of Science panels, and on government task forces seeking to advance security and privacy.
 - Testimony and informal advice to Congress and state and federal government agencies on information security, identity theft, and links between fraud and national security.
 - An ongoing speakers series that brings faculty and students on the Bloomington and IUPUI campuses together with leading researchers and practitioners from academia, industry, and government.
 - The annual Indiana Higher Education Cybersecurity Summit.
- For further information, visit the center's Web site at www.cacr.iu.edu