



Grand Theft Identity

Be careful, we've been told, or you may become a fraud victim. But now it seems that corporations are failing to protect our secrets. How bad is the problem, and how can we fix it?

By Steven Levy and Brad Stone
Newsweek

July 4 issue - Millions of Americans now have a new reason to dread the mailbox. In addition to the tried-and-true collection of Letters You Never Want to See—the tax audit, the high cholesterol reading, the college rejection letter—there is now the missive that reveals you are on the fast track to becoming a victim of identify theft. Someone may have taken possession of your credit-card info, Social Security number, bank account or other personal data that would enable him or her to go on a permanent shopping spree—leaving you to deal with the financial, legal and psychic bills.

Deborah Platt Majoras got the pain letter last week, from DSW Shoe Warehouse. Hers was among more than a million credit-card numbers that the merchant stored in an ill-protected database. So when hackers busted in, they got the information to buy stuff in her name—and 1.4 million other people's names. "It's scary," she says. "Part of it is the uncertainty that comes with it, not knowing whether sometime in the next year my credit-card number will be abused." Now she must take steps to protect herself, including re-examining charges closely, requesting a credit report and contacting the Federal Trade Commission to put her complaint into its extensive ID-theft database. The latter step should be easy for her, since Majoras is the FTC chairman.

Somewhere, Willie Sutton is smiling. Sutton was the sly swindler who, when asked why he robbed banks, was said to reply, "Because that's where the money is." Today the easy money is still in banks—databanks: vast electronic caches in computers, hard disks and backup tapes that store our names, Social Security numbers, credit-card records, financial files and other records. That information can be turned into cash; thieves can quickly sell it to "fraudsters" who will use it to impersonate others. They visit porn sites, buy stereo systems, purchase cars, take out mortgages and generally destroy the credit ratings of innocent victims, who may be unable to get new jobs, buy houses or even get passports until the matter is painstakingly resolved. And since the crime is all done remotely, modern ID thieves suffer little of the risk that Sutton shouldered a half century ago when he robbed banks with a machine gun.



• Be careful, we've been told, or you might be a fraud victim. Now it seems that corporations are failing to protect our secrets. How bad is the problem, and how can we fix it? **BY STEVEN LEVY AND BRAD STONE**

Illustration by Viktor Koen for Newsweek

We've become accustomed to the digital grease that smooths transactions, loans and eBay bids, but worries about identity theft quietly shadow us, often leading us to restrict our activities and be extra careful with our credit cards and personal information. In recent weeks, though, there's been something different, a cascade of reports about big break-ins and bumbles where the booty is our secrets. Suddenly things seem out of control: instead of losing our identities one by one, we're seeing criminals grabbing them in massive chunks—literally millions at a time. "It only makes sense that criminals would go where information is collected," says Martha Stansell-Gamm, head of the DOJ's computer-crime division. The biggest heist of all may have been the one revealed last week, where an Atlanta-based company called CardSystems was lax in protecting the credit cards from transactions it processed. As a result, a possible 40 million Discover, Visa, MasterCard and American Express numbers (along with the secret code numbers

printed on the actual cards, which makes it easier to counterfeit new versions) were exposed to hackers who have already begun the process of turning the digits into cash and prizes.

"Over the last nine years, criminals have gotten a better understanding of the power of information," says Rob Douglas of PrivacyToday, a security consulting firm. "Instead of selling drugs, so much can be made so quickly with identify theft, and the likelihood of getting caught is almost nil." The Department of Justice has reprioritized to fight the plague, but it's a big challenge; Avivah Litan of research firm Gartner Group speculates that fewer than 1 in 700 identity crimes leads to a conviction. This goes a long way toward explaining why it's the fastest-growing crime of this century. Chairman Majoras, now suffering anxiety simply because she bought some shoes, has testified before Congress that crooks rack up \$53 billion a year in ID theft. Consumers are stuck with \$5 billion directly, but the rest of it is mainly paid by retailers and businesses—which pass it back to us in higher prices.



Losing your credit card can be a huge hassle, but the law limits losses. In more distressing forms of ID theft, someone swipes not just your card but also your entire financial persona. Jamie Llanes, a 28-year-old mother of six in Chetek, Wis., has been living a nightmare since last September, when she was turned down for a loan because of a "substantial address difference" in her file—namely, a house in her name in Rialto, Calif., a state she had never set foot in. She also discovered that her doppelgänger had taken out an \$8,700 car loan, and paid it back "to make my credit boost up so they could buy the home." Meanwhile, Llanes can't even get approved for a Victoria's Secret card, and the local police won't help her.

"To a certain extent you can't do anything," says Essita Holmes, a D.C. public defender whose years of shredding documents seemed wasted after ID thieves established a phony bank account in her name to cash bad checks at Target and Wal-Mart. "We're all victims in waiting."

For years, the primary cause of ID theft has been good old-fashioned analog crime. Thieves rifle mailboxes, snatch purses and dive into Dumpsters for discarded bank statements or credit-card receipts. More recently, we've seen a plague of "phishing"—sending bogus e-mails that look like they come from legitimate companies, asking us to supply supposedly lost or outdated personal information. Last week phishers, trying to capitalize on the news, sent out e-mails supposedly from MasterCard, asking people to update their information. "They played on the fear that consumers had when the announcement was made," says Susan Larson of SurfControl, an Internet-security firm.

By now, savvy computer users know the requisite defense against a phishing attack: never respond to a request for your personal information. This wisdom is part of the standard tool kit of protections against ID theft. Check your credit-card bills with an eagle eye. Request your credit report. Shred your information with the fervor of an Enronite. Every aspect of this regime makes perfect sense for each of us to protect the identity we call our own. But when it comes to companies charged with safeguarding millions, sometimes even billions, of records, what do they do?

They leave it unencrypted on computers, where malicious hackers get hold of it. The DSW Shoe Warehouse is far from the only hacked database owner. According to an FTC consent order, BJ's Wholesale Club, a Massachusetts-based firm operating big-box stores and gas stations, not only failed to encrypt, but stored records in violation of bank-security rules, didn't use a firewall to prevent wireless intrusions and protected the information with the easy-to-guess default passwords that came with the system. Result: credit cards ripped off in early 2004 were used to fraudulently charge millions in goods.

They inadvertently sell it to crooks. ChoicePoint is an information broker that keeps, or can electronically access, 19 billion records on American consumers, almost certainly including you. It prides itself on the security of its databases—but that didn't matter when it sold the secrets of at least 145,000 consumers to a fake company last year, including the Social Security number of Kei Kishimoto, a Boston biotech researcher. ChoicePoint gave Kishimoto a year of free credit monitoring, but then he's on his own. "Those numbers could be in a million places by now," he says.

They pack it in boxes and put it in a UPS truck. That's what CitiFinancial, a unit of Citigroup, did with the financial secrets of 3.9 million customers last May. The box never arrived at its destination, and now CitiFinancial's telling customers that their identities are at risk. For Jessica Jerwa, a Seattle paralegal, who's a previous victim of ID theft, learning that her records were lost by Citi was a scary *deja vu*.

They leave it on laptops that get stolen. Last March at UC Berkeley someone made away with a computer holding personal information of almost 100,000 grad students and applicants.



The characters: Victims, activists and prosecutors tell their stories.

They don't monitor what insiders may do with it. In April, Hackensack, N.J., police arrested eight employees at Bank of America, Wachovia, PNC and Commerce banks for selling customer-account numbers to an unlicensed collection agency run by a convicted criminal. The operation snared data on more than 676,000 people, including customers from six additional banks.

They just plain lose it. Bank of America is still looking for backup tapes with information on 1.2 million government workers, discovered lost in December. Maybe they're in the same place as the records Time Warner lost in March, containing 600,000 missing records on past and current employees and their families.

One reason we're hearing about all these breaches is that a 2003 California law required companies for the first time to disclose the failures that affect residents of that state. "Before the disclosure law, we were in the dark," says Beth Givens, head of the Privacy Rights Clearinghouse. "The general public is just now learning about how insecure the computer networks are that hold our sensitive personal information."

Without that law, we may not have even heard about the mother of all breaches, CardSystems. The privately held company processes an estimated \$15 billion credit-card transactions a year (between the merchant and the bank). In direct violation of its agreement with MasterCard and Visa, CardSystems retained 40 million credit-card numbers "for research purposes," as its CEO John Perry initially told the press. These were sucked out of the system by digital invaders. CardSystems's clients admit that protection was lax: "Obviously there were deficiencies and other issues," says Josh Peirez, head of government affairs for MasterCard. Since the break-in, CardSystems has reportedly installed a new "intrusion-prevention product" (hey, thanks).

Obviously, an elaborate infrastructure of crime has emerged to collect and distribute stolen records. "It's not the lone gunman of the past," says Chris Painter of the Department of Justice. "There are highly structured criminal organizations operating." When it comes to attacking databases, malicious hackers either use automated software "bots" to methodically probe the Internet for vulnerable databases or target companies that are likely to harbor honey pots. Most often, they enter systems through preventable security flaws, like guessable passwords (example: "Dave" or the default password that came with the program) or known vulnerabilities in software.

Once records are stolen, they are passed on or sold in fleeting digital dark alleys—chat rooms or instant-messaging sessions where transactions are quickly, stealthily enacted. Sometimes the crooks are sufficiently brazen to post their offerings on Web sites that are sort of fraudster eBays. At one site posted by a member of the Shadowcrew organization (which was shut down by the Feds last year in the biggest ID-theft bust to date, code-named Operation Firewall), \$200 gets 300 credit cards without the CW2 security codes printed on the back of the card. If you want card numbers with the security code, it will cost you \$200 for 50 of them. If you want the fraudster equivalent of a Happy Meal—a card packaged with the owner's Social Security number and date of birth—that will cost you \$40 apiece.

After fraudsters buy the purloined numbers, they commonly use them to grab goodies as fast as possible. It's kind of a high-tech form of supermarket sweepstakes, where the crook keeps stealing until the fraud-management software of the credit-card companies kicks in. "The method is smash-and-grab," says Cybertrust VP Bryan Sartin. "The turnaround time is amazing."



As bad as the recent exposures have been, they may well wind up helping spur some very long-needed reform. Though identity theft is a devilishly difficult crime to fight, the key to fighting these huge cyber-raids is making the databases that hold our private records more secure. "We have not built a culture of strong security around our data," says FTC chairman Majoras, and a big reason is that the companies charged with safeguarding the information don't suffer the consequences when it's compromised. For instance, ChoicePoint CEO Derek Smith got a \$1.8 million bonus for the company's performance last year—*after* it sold the information to thieves. And credit-card firms that use CardSystems are continuing to work with the company. "They've been extremely cooperative in

working with us and other entities to address the vulnerabilities in their system," says MasterCard spokesperson Sharon Gamsin.

Sen. Dianne Feinstein is sponsoring a bill that would set a national standard for mandatory disclosure when consumer records are compromised. (The American Bankers Association opposes it: "Unnecessary warnings could create a cry-wolf attitude," says the lobbying group's John Hall.) But that's only a first step. "The notification law works by shaming the companies, and while that can be a good incentive, it's dependent on publicity," says Bruce Schneier, founder of the Counterpane security firm. "Since we're seeing so many big breaches, there's a higher standard for something to be newsworthy."

A stronger solution would make the companies liable for its failings. Sens. Charles Schumer and Bill Nelson hope to pass a bill that, among other things, would slap fines on companies that lose records. Other approaches would invoke penalties if companies did not follow what are known as best practices in protecting information, like regular security audits and use of encryption. (White House Press Secretary Scott McClellan says ID theft "is a major issue for the administration," but while the president did sign legislation for tougher sentencing of credit-card crooks, the Bush team has not thrown its support behind efforts to force tighter security on the handling of personal data.) If Congress doesn't do it, maybe the legal system will; a class-action suit is underway in the ChoicePoint breach, and Melvyn Weiss (famous for his stock-fraud litigation) says "the phone has been buzzing" with potential clients whose secrets were lost by corporations. In general, anything that increases the cost of losing information to the company, as opposed to the consumer, would give firms an incentive to protect consumer secrets as closely as they do their cash. (Government databases should also be fortified; an April GAO probe found that the IRS's computers were vulnerable to data thieves.)

Identity theft would also be more difficult if companies weren't so dependent on using people's Social Security numbers, the skeleton key for ID crooks. "It was never meant to be an identifier to the general public," says Rep. E. Clay Shaw Jr. of Florida, who for the fourth time is introducing a bill to limit its use. And Senator Feinstein would like to give consumers the power to keep their records out of databases. "Companies have no right to use your personal data without your permission," she says. Industry advocates claim that this would severely slow down the rapid pace of commerce we're accustomed to, but the "opt-in" approach is the law in Europe.

Each time we hear of another huge data breach—and each time a form letter goes out telling someone that his or her secrets were exposed—the pressure increases to tighten up security and fight the ID crooks. But change, if it comes, will come too late for Daniel Bulley, who's spent months trying to distance himself from a home he never owned, a job he never held and a portfolio of credit cards and accounts he never opened. Bulley is angry—at the crooks, at the cops (no one would investigate his case) and the corporations who let his information fall into evil hands. He's especially steamed at the billion-dollar industry that has emerged to sell people protection against data theft—run by parts of the same industry that fails to protect the information in the first place. "Corporate America needs to realize it needs to be tighter with our personal information," says Bulley. "Why should we pay them to do their job right?"

Reported by William Lee Adams, Holly Bailey, Jennifer Barrett, Juliet Chung, Temma Ehrenfeld, Charles Gasparino, Andrew Horesh, Nicole Joseph, Susannah Meadows, Ben Whitford and Kathryn Williams