

STOP THIEVES FROM



STEALING YOU

At a time when your good name and credit are used to judge you as never before—from whether you'll get that next job to the rates you'll pay for insurance policies—your good name and credit have never been more at risk.

Identity theft—the fraudulent use of your name and identifying data by someone else to obtain credit, merchandise, or services—claimed seven million victims in the U.S. last year, according to a recent survey by Privacy & American Business, a publication of the Center for Social & Legal Research, a nonpartisan think tank. That's 10 times as high as past estimates. Canada, Japan, and the United Kingdom are among those countries also reporting ID-theft epidemics.

It is an equal-opportunity crime, affecting victims of all races, incomes, and ages. Overall, more than 33 million Americans, about 1 in 6 adults, say they have had their identities used by someone else sometime since 1990, the survey found. Indeed, the Department of Justice says ID theft is the nation's fastest-growing financial crime, and the damages to consumers are becoming ever more pernicious.

Margaret Murray, a disabled homemaker from Spartanburg, S.C., was arrested in front of her son after a thief passed bad checks in her name. Frances Green, a beautician from Jamaica, N.Y.,

discovered that the house she was about to buy had already been sold—to an ID thief posing as Green who, with a phony seller and fake lawyers, defrauded the mortgage company and ruined Green's credit. Identity fraud has become a major element in crimes ranging from international drug trafficking to terrorism; Al Qaeda operatives in Spain used stolen credit and telephone cards and false passports and travel documents to open bank accounts and pay for travel and

communication abroad, an FBI agent testified before a congressional subcommittee last year.

Many victims don't learn of the crime for a year or more, only after something goes terribly wrong, because thieves often shield their actions by using a different address when they open new accounts in the victim's name. Typically, federal laws cap monetary losses to consumers, but even in routine cases, it takes victims two years on average to clear their names, according to the Privacy Rights Clearinghouse, a nonprofit advocacy group. Some victims say that during that time, they haven't been able to get a car loan or a mortgage; they couldn't even use their cell phone. Moreover, all consumers end up paying for ID theft: The \$4.2 billion that businesses will lose this year to the crime, a figure expected to mushroom to more than \$8 billion by 2006, they recoup by charging you higher fees and prices.

Identity theft is a problem largely because financial institutions, merchants, credit bureaus, and the government do not adequately safeguard vast databases and other records containing consumers' sensitive information, making it relatively easy for thieves—often insiders—to access these data. Many institutions use Social Security numbers when other identifiers would suffice, fail to notify consumers

CR Quick Take

Seven million Americans were victims last year of ID theft. The fastest-growing financial crime, it involves the fraudulent use of someone else's identity to get credit or merchandise.

- Victims typically lose \$800 and spend two years clearing their name.
- Your best defense: Order your credit-bureau report annually from each of the three major credit bureaus and check for errors and bogus accounts.
- ID theft insurance is typically not worth paying for. And credit-monitoring services don't prevent the crime.
- For tips on how to prevent ID theft and what to do if you become a victim, see pages 16 and 17.

when security breaches occur, and provide little help or recourse for consumers stuck cleaning up the mess.

"ID theft usually occurs not because of the carelessness of the individual consumer, but because of the carelessness or vulnerability of the organizations they deal with, including the government," says Robert Richardson, editorial director of the Computer Security Institute, a research and training organization for computer- and network-security professionals.

Many businesses don't bother to report problems. A recent nationwide survey of 530 large and small businesses by the San Francisco office of the FBI and the Computer Security Institute found that 56 percent said they had experienced the "unauthorized use" of a database, but only 30 percent had reported the incident to law enforcement. Prior years were even worse; while the percentage of break-ins was roughly the same, only 17 percent were reported.

HOW CROOKS GET YOUR ID

All that ID thieves really need to open credit or bank accounts under your name or to drain your existing accounts are three pieces of information: your full name, Social Security number, and date of birth. They can get by with less when financial institutions fail to check identifying information. What follows are seven ways in which thieves can get information about you and how to stop them:

FALSELY ARRESTED

NAME: Margaret Murray, 48, homemaker, Spartanburg, S.C.

PROBLEM: For months, Murray had tried in vain to get Nations Bank to close a fraudulent checking account that had been opened in her name after her driver's license was lost or stolen. Instead, Murray was arrested at her home, in front of her son, on 13 warrants stemming from bad checks. It took five court appearances in two counties to clear her name. "It was hurtful and embarrassing," Murray says. She recently won a \$300,000 negligence verdict against the bank, which did not verify information before opening the account. Bank of America, successor to Nations Bank, declined to comment for this report.



1 Stealing company data. Millions of identities can be stolen at one time when hackers or insiders break into company databases or commercial Web sites where credit-card information and other personal data are stored. Such databases are proliferating; businesses and governments share everything from marketing lists to property records on the Internet. The federal Gramm-Leach-Bliley Act of 1999, which allows financial institutions to share customer data with affiliated companies, opened the floodgates to the exchange of financial information, some privacy experts say.

These databases are often poorly protected. Last fall, a clerk on a computer-

help desk in a Bay Shore, N.Y., banking-software company was charged with using access codes obtained on the job to download and sell 30,000 credit reports from credit bureaus to other crooks for \$60 each. The resulting losses to victims: more than \$2.7 million, federal prosecutors say.

Earlier this year, Visa, MasterCard, and American Express confirmed that an unknown hacker had accessed 8 million credit-card records, including 3.4 million Visa accounts and 2.2 million MasterCard accounts, from a merchant processor, Data Processors International. The card companies said no information was used fraudulently, but Gartner Financial Services, a technology research and advisory company, estimates that at least 1 percent of those accounts, or 80,000 consumers, will become targets of fraud since stolen credit-card data make ID theft easy.

Last year, the Federal Trade Commission censured online merchant Guess when a 19-year-old novice programmer, testing the site's security before buying a pair of jeans, was able to break in and retrieve 200,000 customer names and credit-card numbers, despite the site's claim of being "secure." A Guess spokeswoman says the company has settled the case with the FTC and upgraded security.

The fix: Financial institutions and other businesses should use encryption and better systems to prevent and detect computer hackers and to control access

ID theft by the numbers

The 10 highest rates of ID theft (numbers are per 100,000 population) occur in:

WASHINGTON, D.C.	123
CALIFORNIA	91
ARIZONA	88
NEVADA	85
TEXAS	69
FLORIDA	68
NEW YORK	67
WASHINGTON	66
MARYLAND	66
OREGON	64

Source: Federal Trade Commission, based on more than 140,000 complaints last year to its Identity Theft Data Clearinghouse.

Thieves often open new credit-card and cell-phone accounts. Reported cases include the following ID frauds*:

Fraud	Percent of cases
Credit card	42
Phone or utilities	22
Bank	17
Employment-related	9
Benefits or government documents	8
Attempted ID theft	8
Loans	6
Other	16

* Many victims experienced more than one fraud.

ID-THEFT PROTECTION SERVICES TYPICALLY NOT WORTH THE MONEY

The most visible response by big business to the epidemic of ID theft has been to roll out insurance and credit products that exploit fear of the crime. Insurers offer ID-theft insurance, which is of dubious value. Credit-reporting agencies and credit-card issuers offer credit-monitoring services, which can be of some help but mostly after you've become a victim.

Identity-theft insurance. Farmers Group, American International Group (AIG), Travelers, Chubb, Encompass, and some credit-card issuers offer these policies. They usually cost \$25 to \$50 per year, and have a maximum benefit of \$15,000 to \$25,000 and deductibles of \$100 to \$250.

Policies generally cover the expenses of cleaning up the crime, including attorney's fees, costs of mailing correspondence, and lost wages. They seldom cover the out-of-pocket loss to the victim, typically about \$800. Given the limited coverage, we don't recommend buying ID-theft insurance.

Credit-report monitoring. This service is pitched by the big credit bureaus—Equifax, TransUnion, and Experian—and by credit-card issuers like Trilegiant. For \$30 to \$150 per year, these companies promise to monitor your credit report and alert you when they receive credit applications or inquiries.



Many experts say, however, that obtaining an annual credit report from each of the three major bureaus, about \$9 apiece, is a sufficient preventive measure for most consumers.

Residents of Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, and Vermont are entitled to a free annual credit report. No matter where you live, you can get a free report if you are a victim of ID theft, unemployed, or have been turned down for credit or a job because of a negative report. California residents who are ID-theft victims are entitled

by insiders, computer security and privacy experts say. But only 10 percent of businesses encrypt their data, according to Avivah Litan, vice president and research director of Gartner Financial Services.

2 Pretexting. E-mail spammers, telemarketers, and even some clerks and salespeople use a false pretense to lure you into revealing personal information. Twice this year, New York City police arrested the same 18-year-old on different versions of this scam. Police say that first, the teenager sent "spoofed" e-mail to AOL account users. Claiming to represent AOL, he requested personal information, including credit-card numbers, to "update" accounts. When AOL users complied, police say he charged more than \$10,000 in merchandise. In the other case, police say he used stolen identities to buy \$30,000 worth of electronics, which he sold on a spoofed Amazon.com Web site.

The fix: Don't use e-mail to send your Social Security number or other personal data. If you must, make sure that you use a secure Internet connection by checking your browser window for a secure-connection icon. We recommend against giving personal information to someone who has called or e-mailed you unsolicited. At least, independently confirm the legitimacy of the request by phoning or e-mailing the company.

3 Dumpster diving. Criminals dig through trash for bills, medical statements, or other papers that can be used to obtain credit or access to your accounts.

The fix: Shred papers containing personal information and preapproved credit offers before discarding them. (See our test results for shredders on the facing page.) Businesses and governments also need to do a better job of disposing of old files. Only California, Georgia, Washington, and Wisconsin have laws requiring businesses to shred files.

4 Mail theft. Individuals and organized rings steal mail from unlocked mailboxes, trying to find letters containing personal information, preapproved credit offers, and "live" checks. Mail theft is a federal crime that carries stiff penalties, but criminals take the risk because the payoff is so large.

The fix: Homeowners and landlords can help prevent mail theft by replacing regular mailboxes with locked boxes.

Businesses should stop using Social Security numbers in routine correspondence and create alternative ID numbers.

5 Account takeover. Thieves use stolen or fake IDs to take over existing bank or credit accounts. They escape detection by forwarding mail to private mailboxes or new addresses.

A recent case involved 17 conspirators, including lawyers and an unlicensed real estate agent. They were indicted in Queens County, New York, in connection with a \$1 million mortgage fraud ring that victimized Frances Green and others whose houses were literally sold or refinanced out from under them. Imposters used fake IDs, including driver's licenses, to pose as the homeowners at staged closings to steal money from mortgage lenders. A real-estate

UNLIKELY VICTIM

NAME: Jerry Coleman, 51, assistant district attorney, San Francisco
PROBLEM: Twice while leading out-of-town ID-theft seminars and a third time locally, Coleman was the victim of "skimming" frauds that charged \$28,000 to his accounts. In the first case, which resulted in several convictions, a hotel clerk swiped Coleman's credit card through a second, hidden card reader that transferred information onto the magnetic strip of a hotel key. The crooks then tried to charge perfume, among other things, to Coleman's account. The other two cases are unsolved. "If you can get them mid-scram, you can bust them," Coleman says.



PHOTO BY ROBERT HOUSER

to a free monthly report for one year.

One instance in which you might consider buying a monitoring service is if you're already a victim of ID theft and want an early warning of new incidents. Consider, however, that even credit-monitoring services may sell data that you provide to them to affiliates, whose databases may not be secure.

ID-theft prevention services have spawned a new scam. Telemarketers and e-mail spammers offering free credit reports ask you to fill out a form with your personal information, which they use to commit fraud against you.

Never accept an offer for free credit reports or credit monitoring. Contact the credit bureaus or your credit-card issuer directly if you want such a service.

office employee may have supplied the victims' names and Social Security numbers to the conspirators, says Detective David Moore of the New York Police Department.

The fix: Better ID verification by mortgage lenders and other financial institutions, such as cross-checking at least four types of identification, would cut down on this kind of fraud, experts say. So would validating Social Security numbers with the Social Security Administration.

6 Skimming. Thieves use handheld magnetic card readers that can be bought on the Internet or improvised to glean personal information off the magnetic strip on credit and debit cards. Sometimes the data are transferred to other magnetic strips to make counterfeit credit cards. The culprits have included waiters, gas station attendants, and store clerks paid by organized-crime rings. Some private automatic-teller machines also have been rigged to skim account numbers and PINs.

The fix: Better employee screening might curb ID theft. Tighter federal regulation of ATMs may also be needed.

7 Raiding your old computer. According to a recent study, MIT graduate students were able to recover sensitive files from hard drives on one-third to half of the used computers they tested. Last year, 150 million computers were discarded, the study found.

The fix: Businesses and individuals should use hard-drive shredding software or remove and destroy hard drives

before discarding a personal computer.

HUGE LOSSES ARE A WAKE-UP CALL

Until recently, identity theft seemed to be regarded by police and many financial institutions almost as a victimless crime. Many victims say they had trouble reporting the crime; local police wouldn't pursue the case. Even today, only 678 of some 18,000 law-enforcement agencies participate in a federal ID-theft database to share tips and leads.

Meanwhile, lenders and merchants chalked up losses to "bad debt," which can be written off on income-tax returns and may cost less than paying for security. Also, businesses have seldom been held liable in lawsuits stemming from ID theft, so there has been little incentive to act.

However, 60 to 80 percent of losses originally classified as bad debt actually may have resulted from ID-related fraud, according to a study by ID Analytics, a San Diego-based supplier of ID-theft-prevention software.

Those losses have been too great to ignore. Financial Insights, a research and advisory company to financial institutions,

says that ID-theft losses, if they continue at today's pace, could reach \$8.5 billion in 2006. The current cost to business is \$18,000 per incident, the FTC says.

Pressure on business and governments to act is also coming from other quarters. The European Union's 1998 European Data Privacy Directive prohibits transfer of personal data to any country that does not have adequate privacy protection. The United States' approach to privacy has been considered inadequate by the EU.

New studies suggest that consumers want businesses and the government to do more, too. In a recent survey of 2,000 consumers by Star Systems, an ATM network, more than two-thirds of respondents said they want financial institutions to verify customers' identities during transactions, even if that is less convenient. Nine in ten said the government should take action concerning ID theft.

Some businesses and governments are taking steps, but critics say more needs to be done.

Tighten security. Visa and MasterCard now require merchants and big banks that issue their branded cards to use

Shredders can foil ID thieves

A shredder can be a valuable tool for getting rid of old documents that contain credit-card account numbers, your birthdate, and your Social Security number—pay dirt for identity thieves.

Our tests of shredders priced from \$15 to \$130, the types sold in office-supply stores, yielded two main findings:

- Cross-cut shredders worked the best. The other kind, strip shredders, were fast but they left long paper bands that could be reassembled relatively easily.

- Expect to pay at least \$40. Less-expensive shredders are typically the strip-shredder variety. At \$130, the top-performing shredder in our tests was the priciest. But it could shred the most per session, 920 pages. The next best shredded less than one-third as much per session, or 270 pages. It is just \$50, however, and you may find that it meets your needs.



Fellowes P400C-2

Quick Ratings Within types, in order of productivity.

Brand & model	Price	Max. sheets/ session	Max. sheets/ pass	Max. run time/ cool down (min.)
CROSS-CUT STYLE <i>Recommended for maximum security</i>				
Fellowes Powershred PS60C-2	\$130	920	8	10-12 on / 20 off
Fellowes Paper Shredder P400C-2	50	270	5	5-7 on / 15 off
Fellowes Paper Shredder P50CM	40	87	5	2 on / 15 off
Aurora Metallic Color Series 5 Sheet Shredder with Wastebasket AS501X-MS	40	74	5	2 on / 4 off
STRIP-CUT STYLE <i>Not recommended for maximum security</i>				
GBC Shredmaster Shredmaster 70S	70	463	8	3 on / 30 off
Tech Solutions 9 Sheet Strip Cut Paper Shredder with Wastebasket TS-2550	15	281	9	2 on / 4 off

secure Internet technology. They're using new identity verification and authentication systems for controlling transactions among customers, merchants, and banks. In addition, both now require member banks and merchants to encrypt personal data stored on their servers.

Credit-reporting agencies say they have spent millions upgrading computer-system security. But they have done little, it seems, to control access to credit reports by unscrupulous employees of credit-bureau clients such as car dealerships, which have been sources of theft and reselling of credit reports.

Robin Holland, senior vice president of customer service at Equifax, says the company inspects clients where its machines are used. If rogue employees of their customers breach security, "I don't see why we would be blamed for that," she says. But Litan, of Gartner Financial Services, says companies could protect against insider threats by limiting those employees with access to credit data.

The largest single source of ID theft is "the corrupt individual on the inside," says privacy expert Alan Westin, president and

AUTHORITIES WOULDN'T LISTEN

NAME: Lance Nail, 37, chairman of the finance department at the University of Alabama in Birmingham
PROBLEM: In July, five years after Nail discovered that his name and Social Security number had been used to open cell phone and utilities accounts in Atlanta, he was finally able to clear up a bogus mobile-phone account. Police in neither Birmingham nor the Atlanta area wanted to investigate. "I wish people would stop calling this a victimless crime," he says. "It takes a lot of time to fix."



publisher of Privacy & American Business.

Indeed, thousands of businesses and government institutions impose too few limits on access to sensitive information, privacy and security experts say. Ligand Pharmaceuticals recently settled a negligence lawsuit in San Diego over ID thefts that occurred when personnel records were left in an unlocked area after Ligand

acquired another company in a merger. A worker discovered the records and used them to open fraudulent credit accounts.

"Too many people have access to the documents," says Margaret Byrne, an attorney who represented the Ligand ID-theft victims. Few managers should have access, and records should be kept under lock and key, she says.

what you can do

Identity theft is often a crime of opportunity. Follow these tips to reduce your chances of becoming a victim.

Check financial statements promptly.

Always review your monthly banking, brokerage, and credit-card statements for accuracy. Report problems immediately.

Watch your credit. Order copies of your credit report every year from each of the three major credit reporting agencies. They are: Equifax, 800-685-1111, P.O. Box 105851, Atlanta, GA 30348; TransUnion, 800-888-4213, P.O. Box 1000, Chester, PA 19022; and Experian, 888-397-3742, P.O. Box 2002, Allen, TX 75013. Report errors promptly and in writing.

Be stingy with information. Never disclose your Social Security number, birth date, or mother's maiden name unless you initiated the transaction. On paper documents, don't include such data unless required to do so on an official application for employment, financing, or insurance. (Ask employers, schools, and financial institutions to offer alternatives.) Never put such information on personal Web pages or publicly posted résumés or directories.

Just say no. Consider "opting out" of information-sharing at your financial institutions. (Check your company's financial privacy notice, which is mailed annually and usually posted on company Web sites, to find out how.) Also opt out of pre-approved credit offers by calling the Credit Reporting Industry Pre-Screening Opt-Out Number at 888-567-8688.

Travel light. Don't carry ID that contains sensitive data like your Social Security number unless absolutely necessary.

Lock it up. Safeguard your driver's license and other government ID at all times. Lock desks, cabinets, and safes containing such information in your office and home.

Shred and destroy. Before throwing out files containing Social Security numbers, account numbers, and birth dates, shred them with a cross-cut shredder. Destroy CDs or floppy disks containing sensitive data by shredding, cutting, or breaking them. Use hard-drive shredding software or remove and destroy your hard drive before discarding a computer. Just deleting files isn't enough.

Guard mail. Consider using a locked

mailbox or slot to receive mail at home. Deposit mail in postal mailboxes or in the post office to discourage mail theft.

Keep your eye on the prize. Try not to let waiters, sales clerks, or gas-station attendants disappear from view with your credit or debit card, to avoid "skimming." Crooks can use a handheld card reader to copy the information from your card's magnetic strip.

Beware strange ATMs. Avoid using private or strange-looking automated teller machines, because they may be rigged to skim data off your card's magnetic strip. Six- or seven-character PINs (personal identification numbers) are harder to crack than shorter ones, but you may not be able to use them at machines abroad.

No surfing allowed. Watch out for "shoulder surfers" when using pay phones or public Internet access; use your free hand to shield the keypad. Don't use cordless phones to conduct sensitive financial or medical business, because eavesdroppers on other phones and those using eavesdropping equipment may be able to overhear your conversations.



Detect fraud. Some companies that are frequent targets for identity fraud, including cell-phone services, retailers that offer instant credit, and large banks, are investing heavily in systems designed to detect fraudulent credit applications. ID Analytics has designed one that assigns a score like a credit score to a credit application. A high score means the identity of the applicant is probably stolen or fake. The software has detected fraud in 7.5 percent of credit applications.

Under another system, a Social Security number that doesn't correspond to the birth year of the applicant might trigger a warning. But too many merchants still don't check.

Prevent hacking. Systems that monitor an organization's connections to the Internet and that prevent and detect hacking are a must to deter ID thieves and virus attacks, says Richardson of the Computer Security Institute. On the horizon: "trustworthy" computing systems that require authentication and verification before allowing information-sharing among computers or computer networks. The systems work

by not allowing one computer to talk to another unless it knows the "secret handshake."

Such systems are costly, however, Richardson says. They also limit the free exchange of information that many users have come to expect from the Internet.

Pass stricter laws. California leads other states and the federal government with its identity-theft laws. Consumers Union's West Coast Regional Office helped push for many of them.

Many consumer-rights, privacy-rights, and law-enforcement advocates say they want to see other states copy the laws, which do the following:


- Require that consumers be notified of security breaches that could compromise their personal data, including Social Security numbers.
- Entitle fraud victims to a free credit report every month for a year after they notify credit-reporting agencies that they have been victims of fraud.
- Require individuals requesting birth or death records to provide proof of identity and to sign a form indicating the reason for the request.

- Allow customers to freeze their credit reports if they have been victims of fraud. This requires credit-reporting agencies to get permission from consumers before disseminating their credit reports to lenders. Also, state law requires credit issuers to honor fraud alerts on files and to deny new credit requests until the consumer is notified. Texas enacted a similar credit-freeze law, which Consumers Union supported.

- Require law-enforcement officials to take reports of identity theft in the jurisdiction where the victim resides.

- Limit the use of Social Security numbers.

Proponents say such laws go a long way toward preventing identity theft and helping victims to limit the damage. In addition, more than 20 bills concerning identity theft are pending in Congress.

"Anyone who stores information needs to do more," says Eliot Spitzer, New York Attorney General, whose wife, Selda Wall, was an ID-theft victim. But, he added, "federal legislation is going to be necessary." 

Build a wall. Install firewalls and virus-detection software on your home computers to discourage hackers.

Log off. Quit your browser and log off after using public Internet-access computers in libraries, Internet cafes, and the like. Don't pay bills, bank, or conduct other financial transactions on public computers. If you have a high-speed Internet connection at home, unplug the computer's cable or phone line when you are not using it to discourage hackers.

Deal only with reputable Web sites. Check privacy and security policies of Web sites before making purchases, trading stocks, or banking online. A professional-looking Web site is no guarantee of security. Don't respond to unsolicited e-mail requests for personal information.

Get complicated. Consider password-protecting all your bank and brokerage accounts. Create passwords at least eight characters long.

Check your workplace. Ask how your employer safeguards employee records. Request that Social Security numbers not be used as employee ID numbers.

IF YOU BECOME A VICTIM

Report the crime. Filing a report with your local police and keeping a copy yourself will make it easier to prove your case to creditors and merchants and may help you build a lawsuit if you have to sue to recover losses or clear your name later. In some states, you may have to report the incident in the jurisdiction where the fraud occurred, such as the location of the store where the thief charged merchandise to your account, even if that is not where you live.

File a complaint. The Federal Trade Commission (877-ID-THEFT; TDD, 202-326-2502) investigates interstate and Internet fraud. Download a copy of an ID theft affidavit from the FTC's Web site at www.consumer.gov/idtheft to help you notify merchants, financial institutions and credit bureaus. For fraud involving stolen mail, also file a complaint with postal officials at www.usps.com/postalinspectors/fraud/MailFraudComplaint.htm.

Alert credit-reporting agencies. Use the FTC ID-theft affidavit mentioned above to help you do this. Call TransUnion, 800-680-7289; Experian, 888-EXPERIAN; and Equifax, 800-525-6285, to get addresses and instructions.

Ask to have your account flagged with a fraud alert, which asks merchants not to grant new credit without your explicit approval. Keep copies of all your correspondence.

Notify banks, creditors, and utilities. Close accounts that have been used by thieves. Choose new passwords and PINs for all your accounts and don't use your mother's maiden name as a password. Notify merchants that issued credit or accepted bad checks in your name; use your police report or FTC affidavit as backup.

Order your credit report each year. Get credit reports from all three credit bureaus, and study them closely. Some victims say that it took years to clear their credit files and that new credit was sometimes granted in their names without their permission even after fraud alerts were placed on their accounts.

Seek other help. To share your views about identity theft with your state or federal legislators, visit Consumers Union's public-policy Web site at www.consumersunion.org. For other information, check out the nonprofit Identity Theft Resource Center at www.idtheftcenter.org and the Privacy Rights Clearinghouse at www.privacyrights.org.