PREVENTING IDENTITY THEFT:

a GUIDE for CONSUMERS

NATIONAL CRIME PREVENTION COUNCIL

NCPC

BJA Bureau of Justice Assistance
Office of Justice Programs ■ U.S. Department of Justice

NATIONAL CRIME PREVENTION COUNCIL

The National Crime Prevention Council (NCPC) is a private, nonprofit tax-exempt [501(c)(3)] organization whose primary mission is to enable people to create safer and more caring communities by addressing the causes of crime and violence and reducing the opportunities for crime to occur. NCPC publishes books, kits of camera-ready program materials, posters, and informational and policy reports on a variety of crime prevention and community-building subjects. NCPC offers training, technical assistance, and a national focus for crime prevention: it acts as secretariat for the Crime Prevention Coalition of America, more than 360 national, federal, state, and local organizations committed to preventing crime. It hosts a number of websites that offer prevention tips to individuals, describe prevention practices for community building, and help anchor prevention policy into laws and budgets. It operates demonstration programs in schools, neighborhoods, and entire jurisdictions and takes a major leadership role in youth crime prevention and youth service; it also administers the Center for Faith and Service. NCPC manages the McGruff® "Take A Bite Out Of Crime®" public service advertising campaign. NCPC is funded through a variety of government agencies, corporate and private foundations, and donations from private individuals.

BJA Bureau of Justice Assistance
Office of Justice Programs ■ U.S. Department of Justice

This publication was made possible through Cooperative Funding Agreement No. 2002-DD-BX-K004 from the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. Opinions are those of NCPC or cited sources and do not necessarily reflect U.S. Department of Justice policy or positions. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime.

Printed in the United States of America
July 2005

National Crime Prevention Council
1000 Connecticut Avenue, NW, Thirteenth Floor
Washington, DC 20036-5325
202-466-6272
www.ncpc.org

ISBN 1-59686-011-1

INTRODUCTION

Few crimes have made people more anxious more quickly as the sudden onslaught of identity theft.

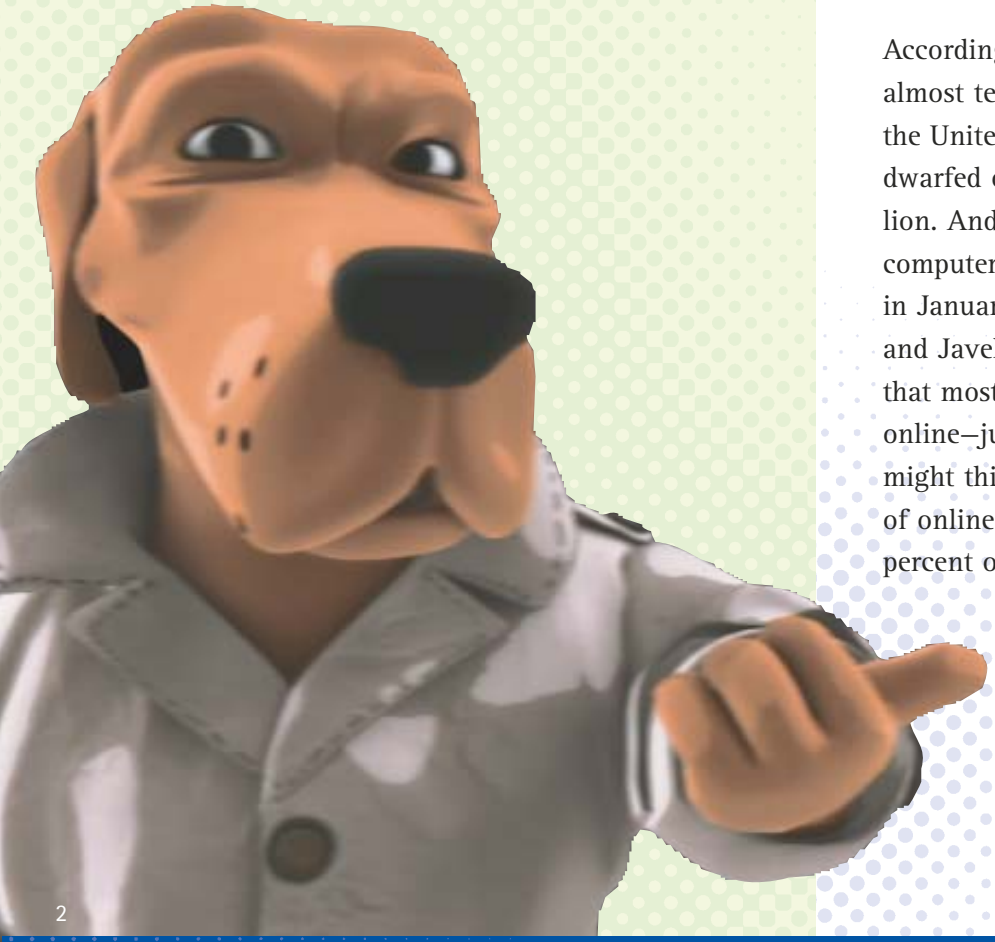
It's in the newspapers every day and on the news every night. People are worried that someone's going to run up charges on their credit cards or fleece their bank accounts while their backs are turned. And there's some reason to worry: All a thief has to do is steal something as basic as a Social Security number to become a real public enemy. And while these crimes are relatively easy to commit, investigating and prosecuting them are complex and time-consuming matters. So it's up to all of us to be identity-smart and make sure we keep this crime from spreading. It's a battle we can win. Follow the tips in this booklet, be careful, and we'll keep a big step ahead of identity thieves. It's up to all of us to prevent identity theft.

—Al Lenhardt, president and CEO, National Crime Prevention Council

WHAT'S IDENTITY THEFT?

The U.S. Department of Justice defines identity theft this way:

"Identity theft is a crime. Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain."



FACTS AND FIGURES

These statistics about identity theft are worth knowing.

According to the U.S. Postal Service, there were almost ten million incidents of identity theft in the United States in 2004, a huge figure dwarfed only by its cost to consumers—$5 billion. And limiting your use of your personal computer may not help much: a study released in January 2005 by the Better Business Bureau and Javelin Strategy and Research reported that most identity thefts take place offline, not online—just the opposite of what many folks might think. In fact, the study found, the theft of online information accounted for only 11.6 percent of identity fraud cases.

Half of all identity thefts are committed by someone the victim knows.

Nonetheless, a rash of headline-grabbing scandals involving thefts of millions of personal records, together with the advent of phishing and pharming thefts (see page 5), may well change that figure dramatically in 2005. One other troubling finding: the study found that half of all identity thefts are committed by someone the victim knows.

In spring 2003, the Federal Trade Commission (FTC)—the federal agency responsible for tracking identity theft—conducted a major study of this crime. Among its findings:

- 12.7 percent of respondents reported that they had been victims of identity theft at some time over the past five years. This implies that at least 27 million Americans had their identities stolen.
- Victims reported that they spent 30 hours, on average, cleaning up after an identity crime at an average cost of $500.

In another study, covering 2004, the FTC reported that of 635,000 complaints registered with the agency, 61 percent involved fraud and 39 percent were identity theft complaints. This study also revealed the following:

- Credit card fraud was the most common form of identity theft, accounting for 28 percent of thefts reported.
- Phone or utilities fraud was next, accounting for 19 percent of identity thefts reported.
- Bank fraud followed, accounting for 18 percent of identity thefts reported.

The FTC also presented some figures about identity theft committed over the Internet. Of 205,568 Internet-related complaints, 90 percent of the victims reported they had suffered a financial loss. The average loss was $1,440.

According to the FTC, the highest reports of identity theft occurred in Phoenix-Mesa-Scottsdale, AZ; Riverside-San Bernardino-Ontario, CA; and Las Vegas-Paradise, NV. While sunny Phoenix and Las Vegas are retirement meccas, the FTC found that of all those who reported being victimized in the United States, only 9 percent were 60 and over while the largest number, 29 percent, were in the 18 to 29 age group.

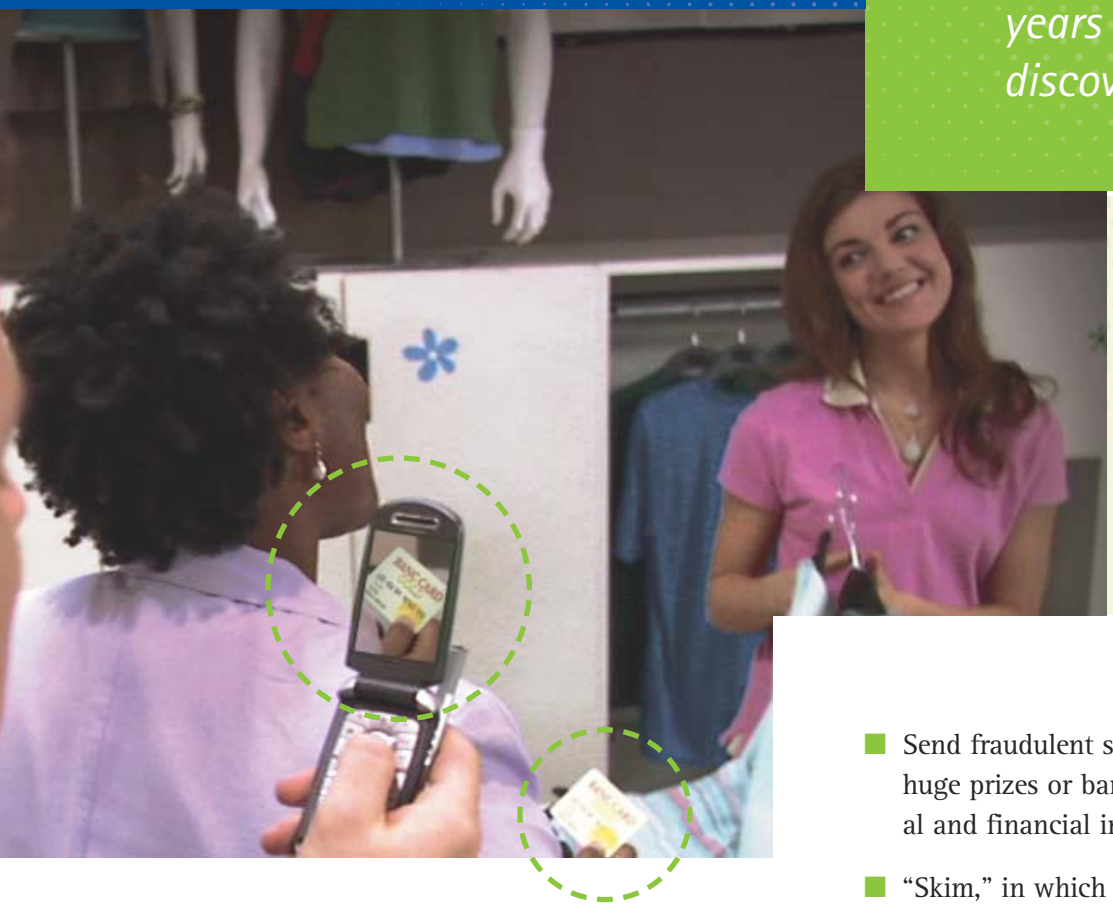
A CROOK'S BAG OF TRICKS

Watch Out for Thefts Like These

Here's a sample of the way identity thieves commit their crimes.

- File a change of address form in your name to divert mail and gather personal and financial data
- Steal credit card payments and other outgoing mail from private, curbside mailboxes
- Lift driver's license numbers, Social Security numbers, phone numbers, or other identifiers from checks
- Steal mail, especially envelopes containing bill payments, from unlocked, unguarded, "out boxes" at work
- Go "dumpster diving" by digging through garbage cans or communal dumpsters in search of cancelled checks, credit card and bank statements, or preapproved credit card offers
- Steal discarded applications for preapproved credit cards and fill them out with a different address
- Steal wallets and purses—and all the credit and identification cards inside them
- Take important documents such as birth certificates, passports, copies of tax returns and the like during a burglary of your house
- Steal Social Security cards
- Steal the Social Security numbers and identities of children who are especially vulnerable because they don't have credit histories and it may be many years before the theft is discovered
- Lift names and Social Security numbers from such documents as a driver's license, employee badge, student ID card, check, or medical chart
- Use personal information from a Who's Who book or a newspaper article
- Use the personal information of a relative or someone he or she knows well, perhaps by being a frequent visitor to their home
- Pretend to be government officials or legitimate business people who need to gather personal information from credit reporting agencies or other sources
- Hack into a computer that contains your personal records and steal the data
- Buy records stolen by a fellow employee who's been bribed
- "Shoulder surf" by watching from a nearby location as he or she punches in a telephone calling card number or listens in on a conversation in which the victim provides a credit card number over the telephone in a public place

Identity thieves may steal the Social Security numbers and identities of children who are especially vulnerable because they don't already have credit histories and it may be many years before the theft is discovered.



- Use the camera in a cell phone to photograph someone's credit card or ATM card while he or she is using an ATM machine or buying something in a store
- "Phish" by sending a legitimate-looking email that directs you to a phony website that looks legitimate and asks for your personal and financial data
- "Pharm," a tactic by which criminals "hijack" whole domains to their own sites and gather the personal and financial data of users who believe they're communicating through their customary service provider
- Send fraudulent spam emails that promise huge prizes or bargains in return for personal and financial information
- "Skim," in which a dishonest merchant secretly copies the magnetic strip on the back of your credit or debit card in order to make a counterfeit card that can then be sold
- Send a fake electronic IRS form to gather personal information and financial data (Note: The IRS never requests information by email.)

More Scams

Financial Crimes

Identity thieves also include crimes like these in their repertoire of dirty tricks.

- They make long-term financial commitments, like taking out mortgages or buying cars, using their victim's credit history.
- They establish, use, and abandon dozens of charge accounts—without paying.
- They may run up huge amounts of debt, then file for bankruptcy in their victim's name, ruining their victim's credit history and reputation.

When Money's Not the Object

Sometimes, the thieves aren't after money. They may use your identity to commit crimes like these:

- They may threaten national security or commit acts of terrorism. The September 11 hijackers used fake IDs to board their planes.
- They use stolen personal information to forge military identification cards, as recently happened at an army base near Washington, DC. This was a potential threat to national security.
- They pile up traffic tickets in your name with no intent to pay them.
- They commit felonies using your identity. Victims of identity theft have been arrested, even jailed, for crimes they didn't commit.
- They may obtain a passport in your name to bring someone into the country for any one of a number of illegal reasons—human trafficking, for example.

HOW TO PREVENT IDENTITY THEFT

Follow these tips to help ensure that you don't become a victim.

Mail Matters

- Don't put outgoing mail, especially bill payments, in personal curbside mailboxes. Use United States Postal Service mailboxes instead, or, better yet, drop off your mail inside a post office.
- Use a locked mailbox with a slot at home, if at all possible.
- Don't put outgoing mail in an unguarded "out box" at work.
- Don't write your account number on the outside of envelopes containing bill payments.
- When you're out of town, have the post office hold your mail for you or have someone you trust pick it up every day.

E-Commerce

- Make sure nobody is standing right behind you when you're using an ATM machine. He or she may be trying to photograph your card number and password with a camera cell phone. Always shield your hand and the screen, even if no one's right behind you.
- Pay your bills online using a secure site if that service is available.
- Don't give out your credit card number on the Internet unless it is encrypted on a secure site.

Personal Finance

- Examine your credit reports from the major national credit reporting firms (see page 10) at least once a year to make sure no one has established credit in your name or is ruining your credit after stealing your identity. The recently enacted Fair and Accurate Credit Transactions Act requires that each of the three major credit reporting agencies provide consumers with a free credit report once a year.
- If you have to give out personal or financial information from a public phone or by cell phone, make sure no one is listening or wait until you're in a more secure location.
- Shred all financial statements, billing statements, and preapproved credit card offers and the like before throwing them in the trash. Cross-cut shredding is best. No shredder? Use scissors to cut documents.

- Minimize the number of identification and credit cards you carry with you. Take only what's absolutely necessary.
- Cancel all credit cards that you have not used in the last six months. Open credit is a prime target if an identity thief spies it in your credit report.
- Write to the Direct Marketing Association to have your name taken off direct mail lists. This will stop the dangerous flow of preapproved credit card offers to your address. This is where to write:

  Direct Marketing Association
  Mail Preference Service
  PO Box 643
  Carmel, NY 10512

- Call the credit reporting industry at 888-567-8688 as an extra measure to stop credit card and insurance solicitations from coming to your home.

Banking

- Use traveler's checks instead of personal bank checks.
- Examine all of your bank and credit card statements each month for mistakes or unfamiliar charges that might be the sign of an identity thief at work.

- Make sure you know when your bills and bank statements normally arrive. If one is late, call to find out why. It may have fallen into the wrong hands.
- Use direct deposit, whenever possible, instead of a paper paycheck.
- Don't have new checks mailed to you at home; pick them up at the bank.
- Be alert if you get a call from someone purporting to be from your bank who asks for personal data to update your "records." This is almost always a scam. If you're in doubt, hang up and call the bank yourself.

Strictly Confidential

- Commit all passwords to memory. Never write them down or carry them with you.
- Don't give out your financial or personal information over the phone or Internet, unless you have initiated the contact or know for certain with whom you are dealing.
- Don't exchange personal information for "prizes." Ask to have the offer put in writing and mailed to you so you can consider it more carefully.
- Give out your Social Security number only when absolutely necessary. Treat it as confidential information.
- Identity thieves have been known to take Social Security numbers from medical charts in hospitals, where the numbers are frequently used as patient identifiers. If you're hospitalized, tell your doctor or nurse to be careful with your chart!
- Destroy the hard drive of your computer if you are selling it, giving it to charity, or otherwise disposing of it. Don't just erase the hard drive; physically remove it.
- Keep your personal information confidential and learn as much as you can about the various kinds of scams being perpetrated to steal your identity. The newspapers are full of tips.

Top Security

- Don't carry your Social Security card with you. Keep it in a safe place at home.
- Don't carry automotive insurance policies in your car. Keep them locked up at home.
- Don't keep your car registration in your car. If possible, carry it in your wallet.
- Keep your wallet in your front pocket so a pickpocket can't take it. Hold your purse close against your body through its straps.
- Burglar-proof your home, then burglar-proof what's inside your home, especially your financial records and important documents (put them inside a locked filing cabinet or safe).

REPAIRING THE DAMAGE

If you're the victim of identity theft, you've got your work cut out for you. Not only will you have to cope with the emotional toll of being a victim of crime, but it will take all the effort you can muster to repair the damage done to your good name and credit. Here's where to start.

Contact the Credit Reporting Agencies

As soon as you know your identity has been stolen, call one of the three major credit reporting agencies. The law requires the agency you call to contact the other two. The agencies will flag your account; this means that any business that wants to view your credit report to give you credit will first have to verify your identity. Upon request, the three agencies will then send you two free reports over the next 12 months. (Beginning in September 2005, the Fair and Accurate Credit Transactions Act requires the three major credit reporting agencies to provide you with a free report once a year regardless of whether you've been a victim of fraud, but you must request them from www.annualcreditreport.com or 877-322-8228.) The three major credit reporting agencies and their toll-free numbers for reporting fraud are listed below.

Equifax	Experian	TransUnion
800-525-6285	888-397-3742	800-680-7289

Work With Your Creditors

If you discover unauthorized charges on your credit report or any billing statement, contact the fraud department of the creditors you believe have been robbed in your name. You have 60 days from the date you normally receive your bill to notify them. If you notify your creditors within this time frame, your loss for unauthorized charges will be limited to $50.

CATCHING THE CRIMINALS

Check Your Bank Accounts

If someone is illegally using your bank account, close the account right away and ask your bank to notify its check verification service. The service will notify retailers not to honor checks written on this account. In most cases, the bank is responsible for any losses. To find out whether someone is passing bad checks in your name, call the Shared Check Authorization Network at 800-262-7771.

If you think someone has opened a new checking account in your name, you can ask for a free copy of your consumer report from Chex Systems (800-428-9623, www.chexhelp.com), the consumer reporting service used by many banks. If your bank doesn't use Chex Systems, ask for the name and number of the consumer reporting service it uses.

Call the Police

As soon as you can, contact your local police or sheriff's department. The police should take your report and give you a copy, or at least the number of the report. You should also consider reporting the crime to your state law enforcement, since many states have recently toughened their laws against identity theft. You will need a police report to pursue your case with creditors who have been victimized in your name. You may also want to contact the office of your state attorney general for consumer fraud information. For a list of state attorneys general, go to www.naag.org.

Be sure to give the police copies of all the documents that support your claim. You may want to provide them with a notarized copy of the Federal Trade Commission's ID Theft Affidavit, available from www.consumer.gov/idtheft.

Because an identity is frequently stolen in one place and used in another, you may also have to contact the police in the place where the crime took place. Your local law enforcement or the creditors affected can tell you if this is the case.

What's the Law?

The federal Identity Theft and Assumption Deterrence Act of 1998 (18 U.S.C. Section 1028) makes it a federal crime when anyone

"knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law."

Other Numbers To Call

- Call the Social Security Administration's Fraud Hotline at 800-269-0271 if your Social Security number has been stolen.
- Call the U.S. Postal Inspection Service if you suspect that a thief has used your mailing address to commit a crime. Call 888-877-7644 for the number of your local office.
- Call the Internal Revenue Service at 800-829-0433 if you believe your identification has been used in violation of tax laws.
- The Secret Service is responsible for investigating financial fraud, but it doesn't investigate individual crimes unless a large amount of money is involved or a ring of thieves is operating. For more information, go to www.treas.gov/usss.
- Report your case to the Federal Trade Commission, which maintains a database that law enforcement agencies use to hunt down identity thieves. To report your theft or to get more information on what to do, call the FTC's toll-free hotline at 877-IDTHEFT.

Tips for Reporting Identity Theft

- Act as soon as you discover the theft. Time is of the essence to prevent further fraud or damage to your credit, and acting quickly may be necessary to protect your rights.
- Keep a record of all conversations with name, agency, phone number, date, and time.
- Keep copies of all emails.
- Never mail originals. Always send out copies, notarized if necessary.
- Use the Federal Trade Commission's ID Theft Affidavit (see page 11) and get it notarized.
- Always use certified mail, return receipt requested, so that you have a record of who received your mail and when.
- Above all, be persistent. It can take time and effort to clean up the mess left behind by the criminal who stole your identity, but only you can do the job.

THREE STEPS TO PREVENTION

This booklet has talked about what you can do to protect yourself against identity theft. But there's also strength in numbers: What else can you and your family, friends, and neighbors do to fight this type of crime? Here are some suggestions.

1. Adopt the measures suggested in this booklet. Set half an hour aside for three days to make the phone calls and take the other steps suggested in this booklet (such as stowing your important papers in a secure place at home).

2. Share this booklet with your family and friends and see if they can come up with other ways to prevent identity theft.

3. Organize a meeting in your school, community center, senior citizen's center, church, or synagogue and invite a police officer to come and tell people about the identity theft problem and what they can do to prevent the crime.

RESOURCES

- The Federal Trade Commission, www.consumer.gov/idtheft
- The Office for Victims of Crime at the U.S. Department of Justice, http://ovc.ncjrs.org/findvictimservices/default.html.
- The U.S. Department of Justice, www.usdoj.gov/criminal/fraud/idtheft.html
- The National Criminal Justice Referral Service, www.ncjrs.org/spotlight/identity_theft/facts.html.
- The Identity Theft Resource Center, www.idtheftcenter.org/vg17A.shtml
- The National Crime Prevention Council's website. Go to www.ncpc.org, click on "What We Offer," go to "What You Can Do," and click on "Protect Yourself Against Identity Theft."

NATIONAL CRIME PREVENTION COUNCIL
1000 Connecticut Avenue, NW, Thirteenth Floor
Washington, DC 20036 **www.ncpc.org**