





The National Crime Prevention Council (NCPC) is a private, nonprofit tax-exempt [501(c)(3)] organization whose primary mission is to be the nation's leader in helping people keep themselves, their families, and their communities safe from crime. NCPC's strategic plan for 2007 through 2011 is centered on four goals: protect children and youth; partner with government and law enforcement to prevent crime; promote crime prevention and personal safety basics; and respond to emerging crime trends. 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 400 national, federal, state, and local organizations representing thousands of constituents who are committed to preventing crime. NCPC also sponsors the National Crime Prevention Association, an individual membership association to promote resources and career development to crime prevention practitioners. It hosts two websites: [www.ncpc.org](http://www.ncpc.org) for adults and [www.mcgruff.org](http://www.mcgruff.org) for children. It operates demonstration programs in schools, neighborhoods, and entire jurisdictions and takes a major leadership role in youth crime prevention and youth 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.



LifeLock, Inc. ([www.lifelock.com](http://www.lifelock.com)) is an industry leader in proactive identity theft protection. Since 2005, LifeLock has been providing consumers with the tools and confidence they need to help protect themselves from identity theft. The company has a strong focus on educating consumers and working with law enforcement and elected officials to better understand the increasing threats of identity theft. A multiple award-winning organization, LifeLock has been recognized by the American Business Awards as Best Overall Company, by AlwaysOn to the Top Global Company 250 list and by Arizona Corporate Excellence as Arizona's Fastest Growing Company.

Copyright © 2010 National Crime Prevention Council

All rights reserved.

Printed in the United States of America

February 2010

National Crime Prevention Council

2345 Crystal Drive, Suite 500

Arlington, VA 22202

202-466-6272

[www.ncpc.org](http://www.ncpc.org)

**F**ew 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 protect ourselves from identity theft.

## 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.”

It can range from unauthorized use of a credit card or check to a comprehensive takeover of another person's identity.

## FACTS AND FIGURES

These statistics about identity theft are worth knowing.

According to the Federal Trade Commission, identity theft was the number one fraud complaint during calendar year 2008. And limiting your use of your personal computer may not help much: a study released by Javelin Strategy and Research reported that in 2009 most identity thefts were taking place offline, not online—just the opposite of what many folks might think. One other troubling finding: the study found that 43 percent of all identity thefts are committed by someone the victim knows.

In 2008, the Federal Trade Commission's (FTC) Consumer Sentinel Network Complaint Data reported

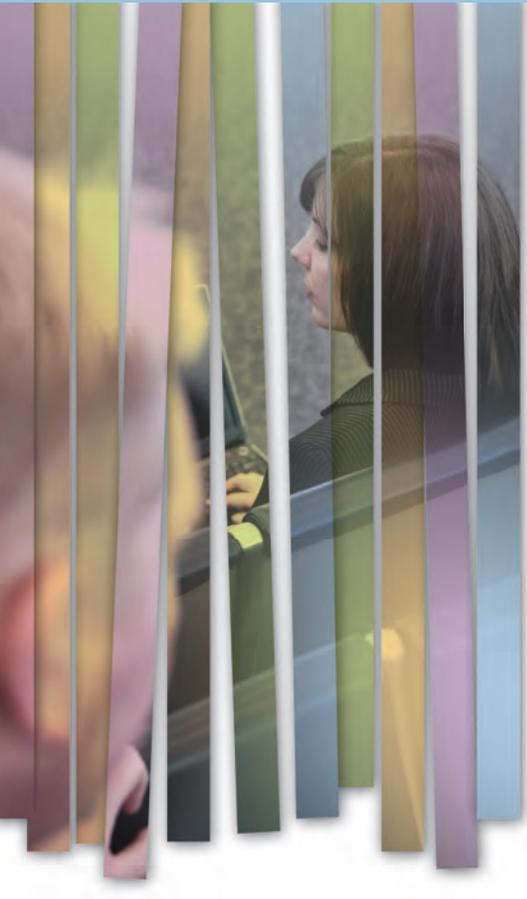
- Twenty-six percent of respondents had been victims of identity theft in 2008.
- Arizona, followed by California and Florida, has the highest per capita rate of reported identity fraud.

- Credit card fraud was the most common form of identity theft.
- Government documents/benefits fraud was the second most common, followed by employment fraud.
- Electronic fund transfer-related identity theft continued to be the most frequently reported type of identity theft bank fraud.



# A CROOK'S BAG OF TRICKS

Watch Out for Thefts Like These



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

- 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 credit card payments and other outgoing mail from private, curbside mailboxes
- Steal mail, especially envelopes containing bill payments, from unlocked, unguarded, “out boxes” at work
- “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
- Take important documents such as birth certificates, passports, copies of tax returns and the like during a burglary of your house
- File a change of address form in your name to divert mail and gather personal and financial data
- Lift driver's license numbers, Social Security numbers, phone numbers, or other identifiers from checks
- 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
- Steal Social Security cards
- Steal through security breaches 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 drivers' licenses, employee badges, student ID cards, checks, and medical charts
- Buy records stolen by a fellow employee who's been bribed

## 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, and then file for bankruptcy in their victim's name, ruining their victim's credit history and reputation.



- Take advantage of peer-to-peer file sharing software such as Limewire
- 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
- “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
- Hack into a computer that contains your personal records and steal the data
- 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
- Send a fake electronic IRS form to gather personal information and financial data (Note: The IRS never requests information by email.)



## 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 happened at an army base near Washington, DC. This was a potential threat to national security.
- They steal insurance information in order to get medical procedures done or to obtain medications.
- 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 PROTECT YOURSELF FROM 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

- Look for evidence that you're doing business on a secure site. In your browser bar, look for https and the lock icon.
- 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 7) 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. You can also get a free credit report through [www.annualcreditreport.com](http://www.annualcreditreport.com).
- 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 or recycling. 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 888-5OPT-OUT as an extra measure to stop credit card and insurance solicitations from people you don't already do business with from coming to your home.
- Consider placing a fraud alert on your account with the three major credit bureaus, freezing your credit, or engaging an identity theft protection service. All of these actions provide an extra layer of security by requiring you to approve the release of your credit information rather than having it supplied automatically. Some of these services are free and some require a small fee.





## Banking

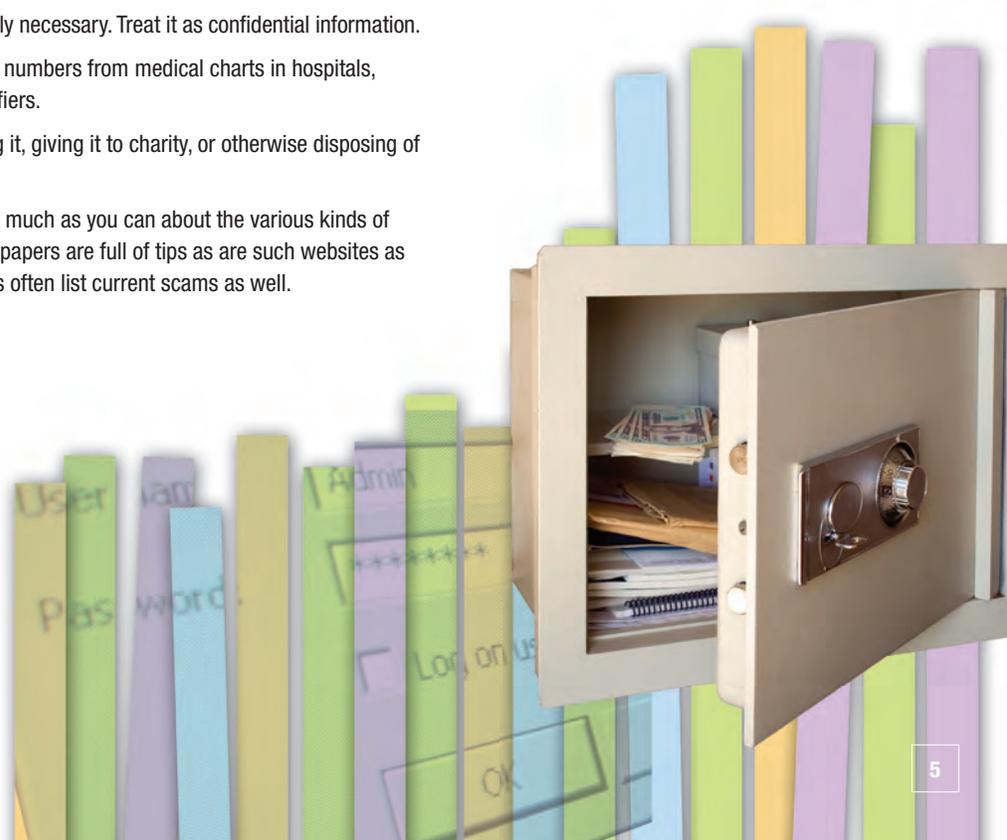
- Use traveler's checks instead of personal bank checks.
- Examine all of your bank and credit card statements each month for mistakes or unfamiliar charges that might be the sign of an identity thief at work.
- Make sure you know when your bills and bank statements normally arrive. If one is late, call to find out why. It may have fallen into the wrong hands.
- Use direct deposit, whenever possible, instead of a paper paycheck that could be stolen from your mailbox.
- 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 at a number you trust.

## 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.
- 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).

## 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 whom you are dealing with.
- 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.
- 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 as are such websites as [www.hoax-slayer.com](http://www.hoax-slayer.com). Local police department websites often list current scams as well.



# REPAIRING THE DAMAGE

If you're the victim of identity theft, here's how to begin to repair the damage.

## Step 1: 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](http://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.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/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.

## Step 2: 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](http://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.





### Step 3: 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. If you have been the victim of fraud, a fraud alert can be placed on your accounts for seven years. 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.) The three major credit reporting agencies and their toll-free numbers for reporting fraud are listed below.



**Equifax**  
800-525-6285

**Experian**  
888-397-3742

**TransUnion**  
800-680-7289

### Step 4: 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.

### Step 5: Report Your Case to the Federal Trade Commission

The FTC 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.



# OTHER NUMBERS TO CALL



- Call the **Social Security Administration's Fraud Hotline** at **800-269-0271** or fill out a report online at [www.socialsecurity.gov/oig](http://www.socialsecurity.gov/oig) 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 **800-275-8777** 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.

## TIPS FOR REPORTING IDENTITY THEFT

- Act as soon as you discover the theft. Time is of the essence to help protect against 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* 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.



# RESOURCES

- The Federal Trade Commission, [www.ftc.gov/bcp/edu/microsites/idtheft](http://www.ftc.gov/bcp/edu/microsites/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](http://www.usdoj.gov)
- The National Criminal Justice Referral Service, [www.ncjrs.org/spotlight/identity\\_theft/facts.html](http://www.ncjrs.org/spotlight/identity_theft/facts.html)
- The National Crime Prevention Council, [www.ncpc.org](http://www.ncpc.org)
- National Organization for Victim Assistance, [www.trynova.org](http://www.trynova.org)
- National Center for Victims of Crime, [www.ncvc.org](http://www.ncvc.org)





**NATIONAL  
CRIME  
PREVENTION  
COUNCIL**

2345 Crystal Drive, Suite 500  
Arlington, VA 22202  
202-466-6272  
[www.ncpc.org](http://www.ncpc.org)