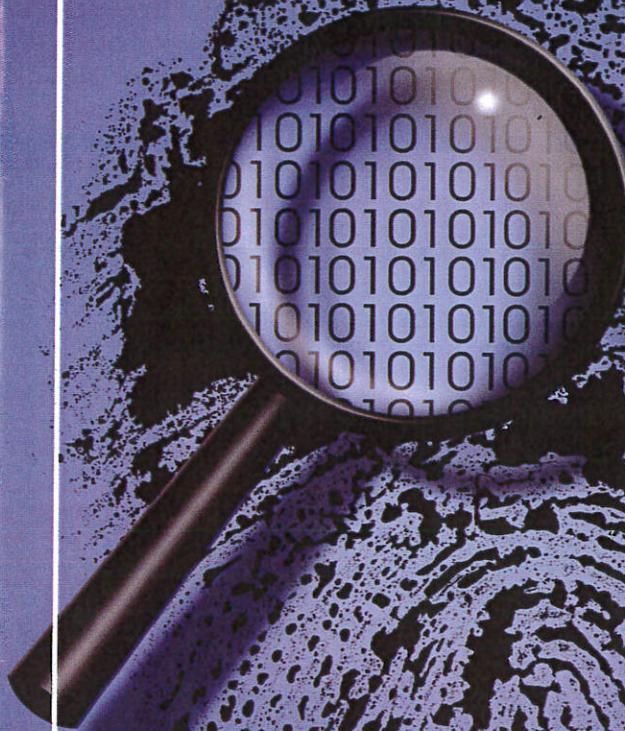


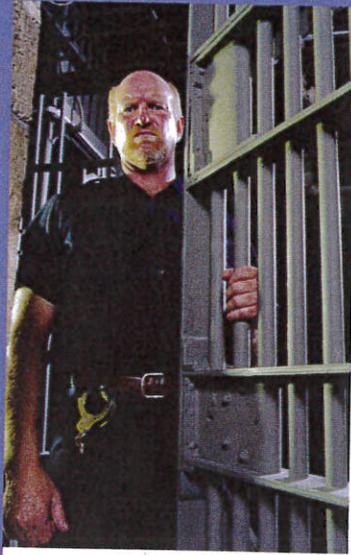
National Child Safety Council

# Identity Theft™



## Protect Your:

- Social Security Number
- Credit Cards
- Bank and ATM Cards
- Address
- Reputation



**More than 11 million people in the U.S. are victims of identity theft, costing over \$54 billion a year.**



## The Crime

**Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number without your permission, to commit fraud or other crimes.**

Under the Identity Theft and Assumption Deterrence Act, a name or Social Security Number is considered a "means of identification." Other forms of identification are a credit card number, cellular telephone electronic serial number, or any other piece of information that may be used alone or in conjunction with other information to identify a specific individual. Identity theft is a federal crime.

## The Penalty

In most instances, a conviction for identity theft carries a maximum penalty of 15 years imprisonment, a fine, and forfeiture of any personal property used or intended to be used to commit the crime.

## The Criminal

Those who commit identity theft usually fall into 3 categories:

1. Someone who knows the victim
2. Someone who is unsophisticated
3. A professional identity thief who works by himself or with an organized group

# Introduction

Unlike your fingerprints, which are unique to you and cannot be given to someone else to use, your personal data CAN be used by others.

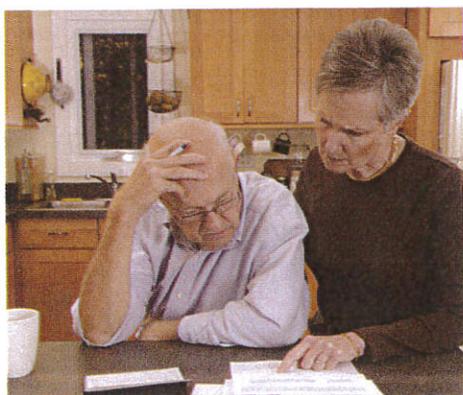
Identity theft has been around as long as people have made monetary and credit transactions without having to be present or show photo ID. However, it has become more prevalent through the use of the Internet.

Considered a **“dual crime,”** identity theft is a crime against the individual whose identity has been stolen and the financial institution or credit company.

Schemes to commit identity theft or fraud also may involve violations of other statutes, such as:

- Credit Card Fraud
- Computer Fraud
- Mail Fraud
- Wire Fraud
- Financial Institution Fraud
- Social Security Fraud

Take the necessary steps to protect yourself. Use this booklet as a quick “how to” guide on how to identify, report, and prevent identity theft.



# Table of Contents

<b>Introduction</b>	1
<b>Table of Contents</b> .....	1
<b>Pretexting: How They Get Your Information</b> .....	2
<b>Becoming You: Ways ID Thieves Use Your Information</b> .....	3
<b>Minimize Your Risk</b>	
Passwords	
Your Mail	
The Internet	
“Free” Offers .....	4/5
<b>Your SSN</b> .....	6
<b>DMV &amp; Signs of Identity Theft</b> .....	7
<b>Credit Cards</b> .....	8
<b>Banking, ATM Card &amp; PIN</b> .....	9
<b>If You Are A Victim</b> ....	10/11
<b>Notifying Law Enforcement</b> .....	12
<b>Prevention</b> .....	13
<b>Information Sharing &amp; “Opting Out”</b> ..	14

This publication is designed to present information about identity theft to employers, employees, and the general public. It is not intended as financial advice. Efforts were made to provide current and authoritative information, but the appearance of information in this publication does not constitute an endorsement of that information by the publisher, nor the accuracy, or the applicability of the information. Consult a financial expert for advice before undertaking any action discussed in this publication.



**Pretexting  
is against  
the law.**

**Victims are left  
with bad credit  
records, trouble  
writing checks,  
difficulty in  
getting loans,  
renting, or even  
obtaining jobs.**



## **Pretexting**

### **How they GET your information!**

Even though you think you have secured your personal information, identity thieves have ways of stealing your data for personal gain, called pretexting by:

- **stealing wallets and purses** with identification on pay stubs, Palm Pilots, health-insurance cards, bank/credit cards.
- **stealing mail** including bank and credit card statements, pre-approved credit offers, telephone calling cards, and tax information.
- **changing your address** to divert your mail.
- **“dumpster diving”** - rummaging through personal or business trash.
- **“shoulder surfing”** - looking over your shoulder while you use the ATM or pay phone to get your PIN.
- **obtaining credit reports fraudulently** by posing as a landlord, employer, or someone else who may have a legitimate need for and legal right to the information.
- **acquiring records** (*business or personal*) at work.
- **searching homes.**
- **using the Internet.**
- **“phishing”** - pretending to be a company you have an account with, directing you to a “spoof site” that looks official, to get you to reveal personal information.
- **“skimming”** - stealing your credit or debit card number by using a special storage device when processing your card.
- **bribing or buying personal information** from “inside” sources. (*From employees with access to credit or service information*)
- **posing as a telemarketer** taking a survey.

**Note:** Some forms of identification are a matter of public record that can be obtained if you have purchased or sold a home, paid taxes, filed for bankruptcy, or any lifestyle change including marriage, births, or divorce. Obtaining this information is not illegal.

# Becoming You

Ways ID thieves  
**USE** your information

Nearly 40% of all  
identity theft victims  
discovered the crime  
within 1 week of the  
start of the misuse.

- 1** They call your credit card issuer pretending to be you, and change the mailing address on your credit card account, then run up charges. Because your bills are being sent to a new address, you may not know right away.
- 2** They open a new credit card account using your name, date of birth, and Social Security number. Then they don't pay the bills and the delinquent account is reported on your credit report.
- 3** They establish phone or wireless service in your name or make unauthorized calls that are billed to you.
- 4** They open a utility account (electricity, heating, cable TV) under your name.
- 5** They open a bank account in your name and write bad checks.
- 6** They file for bankruptcy under your name to avoid paying debts they've incurred under your name, or to avoid eviction.
- 7** They counterfeit checks or use debit cards and drain your bank account.
- 8** They buy, rent, or lease cars or homes by taking out loans in your name.
- 9** They get a job or a driver's license using your Social Security number, birth certificate, or use another form of ID.
- 10** They file a fraudulent tax return using your information.
- 11** They create a criminal record under your name. (In rare instances.)



4 out of 5 people  
believe that  
consumers have  
no control over  
how their personal  
information is used.



**Shred any of the following that you are discarding.**

- Charge receipts
- Copies of credit applications
- Insurance forms
- Physician statements
- Bank checks and statements
- Expired charge cards
- Credit offers you get in the mail

**43% of identity theft victims know who took their information or how it was taken.**

## Minimize Your Risk

- **Adopt a “need to know” approach about giving out your personal information to others.** Before you reveal any information, ask how it will be used, whether it will be shared with others, and ask if you have a choice about the use or confidentiality of your information. Check them out on the Internet directly (*not through a link*) or by calling their customer service number on your bill or in the phone book.
- **Never give out credit card numbers or personal information** on the phone, through the mail, or over the Internet unless you have initiated the contact or know who you’re dealing with.
- **Pay attention to billing cycles.** Follow-up with creditors if bills don’t arrive on time. It could mean an identity thief has taken over your account and changed your billing address.
- **Only carry ID and credit cards or bank cards that you will be using.**
- **Keep items with personal information in a safe place.** Be cautious of roommates, employees, and service technicians.
- **Know who has access to your personal information at work** and that records are in a secure location.

*When opening new accounts, many businesses still ask for your mother’s maiden name. Ask if you can use a password instead. Put passwords on your credit card, bank, and phone accounts. Use a combination of numbers and letters instead of information that could be easily discovered by thieves.*

**Never use:**

- your mother’s maiden name.
- your middle name, your children’s names, or a nickname.
- your birthdate, your children’s birthdates, or an anniversary.
- the last four digits of your SSN or phone or house number.
- a series of consecutive numbers.
- your pet’s name.

**4**

**Passwords**

## Protect Your Mail

- Install a locked mailbox.
- Never leave bill payments in the mailbox for pick up.
- Mail bills and sensitive items at the post office rather than neighborhood drop boxes.
- Never write account numbers on a postcard or outside of an envelope.
- Promptly remove incoming mail from your mailbox.
- Request a vacation hold from the U.S. Postal Service. (1-800-275-8777 or [www.usps.gov](http://www.usps.gov)) when planning to be away.

## The Internet

- Install security software (*firewall protection*) on your computer.
- Never respond to "spam" - unsolicited e-mail offers that promise some benefit after you complete a questionnaire.
- Only shop on secure Web sites. Look for the padlock icon or the "s" in the address. ("<https://>")
- Report suspicious e-mails and Internet scams to the local law enforcement agency.

## "Free" Offers

Never sign up for "free" offers. Junk mail and telemarketing calls obtain too much of your personal information.

### Be leery of:

- warranty/product registration cards.
- joining/donating money to organizations.
- subscribing to magazines or clubs.
- listing your name and number in the phone book.
- sweepstakes contests.



It is a federal crime to steal mail or falsify a change-of-address form.

Read the fine print on applications and order forms.





**Terrorists have been using fake IDs to carry out their terrorist plots.**

**If your SSN has been used, contact the Social Security Administration: (800) 269-0271.**



## Your SSN

### Social Security Number

Your employer and financial institution need your SSN for wage and tax reporting. Other private businesses may ask you for your SSN to do a credit check for a home or car loan. Sometimes, however, others simply want your SSN for general record keeping which **you have the right to refuse**. Ask the following questions to help decide whether or not to provide your SSN:

- *Why do you need my SSN?*
- *How will my SSN be used?*
- *What law requires me to give you my SSN?*
- *What will happen if I don't give you my SSN?*

Keep in mind that businesses may turn you down for a service or benefit if you don't provide your SSN.

- **Only give your SSN when absolutely necessary.** Ask to use other types of ID when possible.
- **Never carry your SSN card with you.** Store it in a secure place.
- **Order a copy of your "Earnings & Benefits" Statement** to see if anyone has used your SSN to earn an income. (800) 772-1213

### Choose a Different ID Number

If your state uses your Social Security number as your **driver's license**, ask to substitute another number. Do the same if your **health insurance company** uses your Social Security number as your **policy number**.



**Contact the check verification company that processes your checks.**

## **DMV** Department of Motor Vehicles

The personal information used to obtain a driver's license is on file at your state's DMV. Many DMVs distribute your information for law enforcement, driver safety, or insurance underwriting purposes, and direct marketing. Contact your state's DMV to find out your options.

### **If You Are A Victim:**

- Contact your state's DMV to see if another license has been issued in your name.
- Inform them that your information has been used fraudulently.
- Put a fraud alert in your DMV file.
- Follow up every few months.

## **Signs of Identity Theft**

**6% of identity theft cases are committed by another family member.**



- ? **Are there accounts in your name that you did not open?**
- ? **Is there inaccurate information on your credit report?** (*Wrong spellings, name or initials, employers, or social security number*)
- ? **Are you missing a bill that you normally receive?** (*Someone could have stolen your mail or changed the address of your bill.*)
- ? **Have you received credit cards that you didn't apply for?**
- ? **Have you been denied credit** for no apparent reason?
- ? **Are you receiving calls or letters from creditors about bills or services that you didn't purchase?**

# Credit Cards

- **Keep a record of your account numbers**, expiration dates, phone numbers, and addresses of each company in a safe place.
- **Never lend your card(s) to anyone.**
- **Do not leave cards or receipts lying around.**
- **Watch your credit cards during transactions.** Get it back as quickly as possible.
- **Void incorrect receipts.**
- **Never sign a blank receipt.** When you sign a receipt, draw a line through any blank spaces above the total.
- **Destroy carbons.**
- **Compare receipts** with billing statements.
- **Open bills promptly.** Reconcile accounts monthly.
- **Report questionable charges promptly** in writing to the card issuer.
- **Notify card companies in advance** of a change in address.
- **Cancel unused credit card accounts.**
- **Contact creditors** about accounts that have been tampered with or opened fraudulently including:
  - credit card companies
  - phone companies
  - other utility companies
  - banks and other lenders
- **If you are a victim of identity theft, alert telephone (and cell), electrical, gas, and water utilities** that someone may try to set up an account using your information.



## If You Are A Victim

1. **Call each credit card company.** Ask to speak with a security or fraud representative.
2. **Follow up with a letter.**
3. **Complete a "Fraud Affidavit" form.**
4. **Close out all of the accounts right away.** Have it processed as "account closed at consumer's request" to keep your previous good credit ratings.
5. **Use new PINs and passwords** for new accounts.
6. **Monitor mail and bills** for evidence.

**Identity theft is a dual crime against both the individual and the financial institution.**

# Banking

## Prevent identity theft:

- **Sign credit or bank cards when they arrive** and carry them separately from your wallet.
- **Never have your SSN printed on your checks.**
- **Do not let merchants handwrite your SSN on your checks.**
- **Pick up new checks at the bank** instead of having them mailed.
- **Store cancelled checks in a safe place.**

## If You Are A Victim:

1. **Cancel the account.**
2. **Set up new accounts/passwords.**
3. **Stop payment** on unauthorized checks.
4. **Contact check verification companies** that handle your checks.

# ATMs

## Automated Teller Machines

- **Shield your hand** when using an ATM.
- **Memorize your PIN** (*Personal Identification Number*). Never carry it in your wallet or purse. Never write it on your ATM card or on the outside of a deposit slip or envelope.
- **Always take ATM receipts** with you.
- **Monitor statements.**

## If You Are A Victim:

- If your ATM card has been misused, report it immediately.
- If it isn't reported within 2 business days after discovery, you could lose up to \$500 in unauthorized withdrawals.
- You risk unlimited loss if you fail to report an unauthorized transfer or withdrawal within 60 days after your bank statement is mailed to you. You could lose all the money in your bank account and the unused portion of your line of credit established for overdrafts.
- Follow-up all calls with a letter.
- Order a new card with a new account.
- Set up a new password or PIN.

**Chexsystems:**  
(800) 428-9623

**Check Center Inquiry:**  
(800) 843-0760

**SCAN:**  
(800) 262-7771

**TeleCheck:**  
(800) 710-9898



**In 1/3 of all ATM card frauds, cardholders wrote their PIN on their ATM card or on a slip of paper kept with their card.**

# If You are a Victim

Contact the fraud department of ONE of the three major credit bureaus **RIGHT AWAY**. (They will contact the other two companies.)

**To report fraud: 1-800-525-6285 and write Equifax.**

To order your credit report: 1-800-685-1111 or write  
Equifax - [www.equifax.com](http://www.equifax.com)  
P.O. Box 740241  
Atlanta, GA 30374-0241

**EQUIFAX**

**To report fraud: 1-888-EXPERIAN and write Experian.**

To order your credit report: 1-888-EXPERIAN (1-888-397-3742)  
or write Experian - [www.experian.com](http://www.experian.com)  
P.O. Box 9554  
Allen, TX 75013

**EXPERIAN**

**To report fraud: 1-800-680-7289 and write Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790.**

To order your credit report: 1-800-916-8800 or write  
Trans Union - [www.transunion.com](http://www.transunion.com)  
P.O. Box 1000  
Chester, PA 19022

**TRANS  
UNION**

1. Tell them you are a victim of identity theft. Ask them to place a "Fraud Alert" in your file.
2. Have them put a "Victim's Statement" in your file asking creditors to call you before opening new accounts or changing existing accounts.
3. Order a copy of your credit report. (Free - if you are a victim and request it in writing, otherwise, the cost can be \$8.50 per copy.)
4. Review the reports carefully for additional fraudulent accounts or activity.
5. Have the credit bureaus contact anyone who has requested your credit report in the last 6 months (2 years for employers) and notify them of your situation.
6. In 3 months, order new copies to verify corrections, changes, and to make sure the fraudulent activity has stopped.
7. Close the account that you know, or believe, has been tampered with or opened fraudulently.
8. Keep a record of the details of conversations and copies of all correspondence.

## DO:

- **Let all parties know that you (as well as creditors and financial institutions) are the victim(s).** Indicate that you are willing to cooperate and have contacted all of the necessary agencies.
- **Keep an extensive log** of who you reported the crime to, what their title was, their direct phone line or extension, and the course of action.
- **Ask for written confirmation of discussions.**
- **Send all correspondence “return receipt requested”** mail to create a paper trail.
- **Keep track of all expenses** accrued while trying to collect and correct your record including phone calls, postage, mileage, time away from work, legal fees, notarization fees, court fees, assistance fees (*including babysitters, accountants, attorney fees*), and medical fees.
- **Attend all court hearings.** Take extensive notes of the participants, content, and outcome.

## DO NOT:

- **pay any bill (or portion) from fraudulent activity.**
- **cover any checks with your own money that you did not write** or that were cashed fraudulently.
- **file for bankruptcy.**
- **allow yourself to be coerced** by any credit company, financial institution, or collection agency into believing that you will be held responsible.



**If you have been a victim, you may want to contact the passport office.**

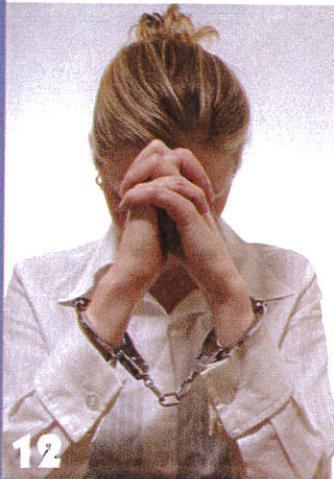
**Less than 12% of identity theft cases begin online.**





**50% of victims filed a police report.**

**13% of identity theft crimes were committed by someone the victim knew.**



## Notifying Law Enforcement

File a report with your local police department and the location where the identity theft took place.

- 1. Give law enforcement as much evidence as possible.**
- 2. Provide a list of the fraudulent accounts.** Make sure they are included in the report.
- 3. Get a copy (or a summary) of the police report** in case the bank, credit card companies, or others need proof of the crime. Even if the identity thief is not caught, having a copy of the police report can help you when dealing with creditors. If you are not allowed a copy of your report, get a letter stating so.
- 4. Keep track of your case number(s)** which will change as your case moves through the judicial system. Note which numbers go with each jurisdiction.
- 5. Provide creditors of fraudulent accounts with a copy of the report.**
- 6. Be persistent.** It is a federal law and a violation of many states' laws to assume someone's identity for fraudulent purposes. Departments may not normally file reports on this type of crime.
- 7. File a complaint with the Federal Trade Commission (FTC).** It does not handle criminal cases, but can provide information and referrals to help resolve problems resulting from this crime.

## Prevention

- **Store your personal information in a secure place at home** especially if you have roommates, employ outside help, or are having work done in your house.
- **Share personal information only with those family members who have a legitimate need for it.**
- **Keep your purse or wallet in a safe place at work.**
- **Monitor your accounts and bank statements each month.**
- **Check your credit report on a regular basis.** Your credit report will contain information about where you work; where you live; the credit accounts that have been opened in your name; how you pay your bills; and whether you have been sued, arrested, or have filed for bankruptcy. **Check the reports for:**
  - misspellings of your name.
  - an incorrect address.
  - discrepancies.
  - activities that you have not authorized.
  - accounts that you did not open.
  - inquiries you did not authorize.



**Order a copy of your credit report from each of the 3 major agencies to review once a year.**

### Should I buy identity theft protection service?

You may want to consider buying an identity theft protection service that notifies the issuers of your credit and ATM accounts if your card is lost or stolen. Many of these services offer credit monitoring, fraud detection, database monitoring, address change notification, and the ability to put a lock on your credit file. **However, it will not stop identity theft from happening.** It simply makes it easier to report and hopefully rectify your accounts.

**FOR MORE  
INFORMATION**

#### **Federal Trade Commission**

Toll-Free Hotline: 1-877-IDTHEFT (438-4338)

TTY: 1-866-653-4261

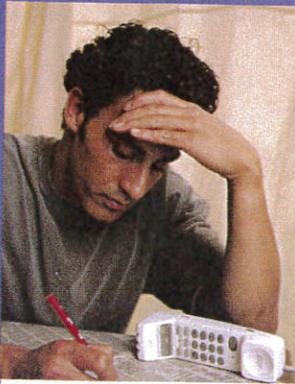
Or Write: Identity Theft Clearinghouse

Federal Trade Commission

600 Pennsylvania Ave., NW

Washington, DC 20580

Online: [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)



**Victims spend about \$400 and 21 hours to regain their credit rating.**

**It is your right to "opt out" of unwanted offers.**



## Information Sharing & "Opting Out"

When you provide personal information to companies, marketing firms, and government agencies, they may use your information to:

- process your order.
- create a profile about you and let you know about products, services, or promotions.
- share with others.

Many companies offer the opportunity to "opt out" of having your information shared with others or used for promotional purposes.

### How can I get off of mail and phone lists?

#### 1. Unsolicited mail:

Direct Marketing Association  
[www.dmaconsumers.org/  
consumersassistance.html](http://www.dmaconsumers.org/consumersassistance.html)

- or -

Direct Marketing Association, Inc.  
1120 Avenue of the Americas  
New York, NY 10036-6700  
Phone: (212) 768-7277 Ext. 1888  
[www.dma.choice.org](http://www.dma.choice.org)

#### 2. Remove any phone number from unwanted telemarketing calls:

National Do Not Call Registry  
1-888-382-1222  
[www.donotcall.gov](http://www.donotcall.gov)

#### 3. Pre-approved offers of credit or insurance:

1-888-5-OPT-OUT (1-888-567-8688)