



*The following information is provided as a service of the Human Services Division.*

## What Is Identity Theft?

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.

### How Identity Theft Occurs

1. **Dumpster Diving-** Rummaging through your trash looking for bills or other information with your personal information on it.
2. **Skimming-** Stealing your credit/debit card numbers by using a special storage device when processing your card.
3. **Changing Your Address-** Diverting your billing statements to another location by completing a change of address form.
4. **Stealing-** Steal wallets and purses, mail, pre-approved credit card offers, and tax information.

### What They Do With Your Information

1. **Credit Card Fraud-** Opening up a new credit card account in your name.
2. **Phone Or Utilities Fraud-** Opening up a phone or wireless account in your name. They may also use your name to get utility services like electricity, heating, or cable television.
3. **Bank/Finance Fraud-** Creation of counterfeit checks, opening up of bank accounts and writing bad checks, cloning ATM cards and making electronic withdrawals, and taking out a loan in your name.
4. **Other Fraud-** Getting a job by using your social security number, renting a house or getting medical services using your name, or giving your personal information during an arrest or court appearance.

**Source:** Federal Trade Commission (2007, October). *About Identity Theft*. Retrieved May, 2007 from <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html>

### Preventing Identity Theft

1. **Change Account Numbers-** If you feel that your bank or credit card numbers have been compromised; contact your bank or credit card company to change

them. Furthermore, make sure that none of your account numbers contain your social security number.

2. **Beware Of Shoulder Surfing-** Don't let anyone hear or see your password. If you must disclose your password in a public setting, do it in an environment where it can't be overheard.
3. **Protect Your Purse/Wallet-** When carrying your purse or wallet, always keep it under your arm and close to your body.
4. **Don't Carry Too Much Info-** Leave any identifiers you don't need at home. This includes your social security card, passport, or birth certificate.
5. **Take Extra Precaution With Credit Cards-** Sign the back of your credit card with "see photo ID". This will prompt anyone running your card to ask for further identification.
6. **Monitor Your Statements-** Check the details of your statements every month. Make sure that there is nothing that you don't recognize and call the credit card grantor if you see anything suspicious.
7. **Don't Bother With Identity Theft Insurance-** There are a multitude of exclusions and many stipulations to reimbursement. Additionally, identity theft insurance seldom provides a resolution to the effects of identity theft, which is what you truly need at the time.

## Avoiding Mailbox Theft

1. **Use The Letter Slots At The Post Office-** If you do mail from your residence, don't indicate your mail with the flag. This is a major attraction for thieves.
2. **Pick Up Mail Promptly-** As soon as you are able to retrieve your mail, do so. Also, don't leave mail in the mailbox overnight.
3. **Have A Trusted Friend Pick-up Your Mail-** If you are away, make sure the person picking up your mail does so in a timely fashion and stores it in a secure place.
4. **Keep Track Of Arrival Dates-** If important bills or paper-work do not arrive when expected, immediately contact the agency.

## Using A Public Computer

1. **Don't Save Logon Information-** Always log off the website by clicking "log out". Simply closing the browser or typing in another web address is not enough.
2. **Don't Leave Computers Unattended-** If you must leave a public computer, log off all programs and close windows that contain personal information.
3. **Erase Your Tracks-** Disable the feature to store passwords and delete your temporary internet files and history. This can be done by simply utilizing the "tools" menu and then clicking "internet options".
4. **Don't Enter Sensitive Information-** If you really want to be safe, avoid typing your credit card number or any other financial or otherwise sensitive information into any public computer.

**Sources:** Microsoft (2006, September). *5 safety tips for using a public computer*. Retrieved May, 2007, from <http://www.microsoft.com/protect/yourself/mobile/publicpc.mspix>

Castle Pines North (2006, December) *Tips for Avoiding Mailbox Theft*. Retrieved May, 2007, from [http://www.cpnhoa.org/pages/news/articles/2005/area/third\\_qtr/mailbox.htm](http://www.cpnhoa.org/pages/news/articles/2005/area/third_qtr/mailbox.htm)

Identity Rehab Corporation (2007, October) *General Security, things to remember when securing your identity*. Retrieved May, 2007 from [http://www.cpnhoa.org/pages/news/articles/2005/area/third\\_qtr/mailbox.htm](http://www.cpnhoa.org/pages/news/articles/2005/area/third_qtr/mailbox.htm)

U.S. Securities and Exchange Commission (2005, September) *How to Protect Yourself Online*. Retrieved May, 2007 from [http://www.cpnhoa.org/pages/news/articles/2005/area/third\\_qtr/mailbox.htm](http://www.cpnhoa.org/pages/news/articles/2005/area/third_qtr/mailbox.htm)

## How To Rebuild Your Identity

### 1. **Place A Fraud Alert On Your Credit Reports**

If you feel that you have been a victim of identity theft, contact the following agencies immediately. You are entitled to order free copies of your credit report. When doing so, look for companies you haven't contacted, accounts you didn't open, and debts you can't explain. Also, check that information like your social security number, address(es), name, and employers are correct.

**Equifax:** 1-800-525-6285; [www.equifax.com](http://www.equifax.com)

**Experian:** 1-800-397-3742; [www.experian.com](http://www.experian.com)

**TransUnion:** 1-800-680-7289; [www.transunion.com](http://www.transunion.com)

### 2. **Close The Accounts That You Know Have Been Tampered With**

Call and speak with someone in the security or fraud department of each company. Follow up in writing, and include documents (not original) of supporting documents. Make sure to keep a record of these documents. Once the issue has been resolved, ask for a letter stating that the company has closed the disputed accounts and has discharged the fraudulent debts. When opening up a new account, avoid using easily available information like your mothers maiden name or your birth date for passwords or pin numbers.

### 3. **File A Report With The Local Police Where The Theft Took Place**

When you file a report, provide as much information as you can about the crime, including anything you know about the dates of the theft, the fraudulent accounts, and the alleged identity thief. If you are told that identity theft is not a crime under your state law, ask to file a Miscellaneous Incident Report.

### 4. **File A Complaint With The Federal Trade Commission**

By doing so, you will provide vital information that can help law enforcement officials across the country track down identity thieves. Their contact information is: **1-877-438-4338** or [www.consumer.gov](http://www.consumer.gov)

Consider the option of applying for a new social security carefully. A new number may not resolve your problem and may actually create new problems.

**Source:** Federal Trade Commission (2007, October). *About Identity Theft*. Retrieved May, 2007 from <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html>