What is Identity (ID) Theft?

Identity theft occurs when an unauthorized party uses your personally identifying information, such as your name, address, Social Security Number (SSN), or credit card or bank account information to assume your identity in order to commit fraud or other criminal acts.

How does identity theft occur?

Identity thieves can steal your personal information directly or indirectly by:

- Stealing your wallets and purses containing identification cards, credit cards and bank information.
- Stealing your mail including credit and bank statements, phone or utility bills, new checks, and tax information.
- Completing a "change of address form" to redirect the destination of your mail.
- Rummaging through your trash for discarded personal data in a practice known as "dumpster diving."
- Taking personal information that you share or post on the Internet.

What can ID thieves do with your information?

- Call your creditors and change your mailing address on your credit card account.
- Open new lines of credit using your personal identification information.
- Establish phone services using your name which are charged to you.
- Open bank accounts in your name and write bad checks.
- Forge checks to wipe out your bank account.
- Apply for auto loans taken out in your name.
- Commit other crimes and then give your name, instead of their own, to the police during their arrest.

What you can you do to prevent ID theft?

Identity theft is on the rise. While there are no guarantees that your identity will not be stolen there are steps you can take to minimize your risk.

- Use passwords on all your credit card, bank, and phone accounts.
- Never keep passwords, "PINs" or your SSN card in your wallet or purse.
- Learn about security procedures in your workplace.
- Never give out personal information on the phone, through mail, or over the internet *unless* you know the receiver and have initiated the contact.
- Guard your mail and trash from theft.
- Shred or destroy discarded financial statements in your trash.
- Give your SSN only when absolutely necessary.
- Keep your purse or wallet in a safe place at work.

How can you protect your personal computer from ID theft?

SSNs, financial records, tax information, birth dates, and account numbers may be stored on you personal computer.
Follow these tips to help keep your personal information safe.

- Update your virus protection software regularly, especially when a new virus alert is brought to your attention.
- Do not download files from strangers or click hyperlinks from people you don't know. This could expose your system to a virus.

- Use a firewall program. This will stop uninvited guests from accessing your computer.
- Use a secure browser to guard the security of your online transactions.

What do you do if you are a victim?

1. Contact the fraud departments of each of the three major credit bureaus. (This information can be found on FTC's ID Theft website or in FTC's ID Theft booklet)
2. Close the accounts that you know or believe have been tampered with or opened fraudulently.
3. File a police report with your local police and/or the police in the community where the identity theft took place.

Where can you find more information on this subject?

The information found in this brochure was derived from FTC's Manual on ID Theft, "ID Theft: When Bad Things Happen to Your Good Name", which was published in September of 2002. It is available at: www.consumer.gov/idtheft/. You can also access more information in the office of the OIG in Rm. 1135.

How can you contact the FTC?

Internet
www.ftc.gov

FTC's ID Theft Hotline
1-877-IDTHEFT (438-4338)

Write
Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Contact OIG

Internet
oig.nsf.gov

Telephone
703 292-7100

Fax
703 292-9158/9159

Write
National Science Foundation
Office of Inspector General
4201 Wilson Boulevard
Arlington, VA 22230

OFFICE OF INSPECTOR GENERAL (OIG)

Identity Theft: What can you do to protect yourself?