USAF ACADEMY LEGAL OFFICE
2304 Cadet Drive, Suite 2100
USAFA, CO 80840
(719) 333-3940

IDENTITY THEFT

---

1. A FEW WORDS ABOUT THIS BOOKLET

This pamphlet is intended to provide a brief overview of identity theft. If you need more detailed information, we encourage you to discuss your specific situation with a legal professional. The attorneys in the base legal office **cannot represent** you in court. Please see the information below for agencies that can assist you with identity theft.

2. WHAT IS IDENTITY THEFT?

Identity theft refers generally to the unauthorized use of personal identifying and financial information to steal your money and your good credit. Identity thieves look for drivers license information, social security numbers, bank account and credit card numbers, calling card numbers, and information on a potential victim's investment accounts, spending habits and even family information (maiden names, children's names or other "personal" information used by many people as passwords on protected accounts). Identity thieves will use that information to empty out existing bank accounts, run up huge charges on your credit cards, and even apply for new credit cards and loans in your name.

A nationwide survey released by the Federal Trade Commission in September 2003, found that identity theft is an even bigger problem than originally believed. According to that survey, more than 9.9 million Americans were the victims of identity theft last year alone, losing a collective $5 billion. According to the FTC database for 2009, complaints by Colorado victims of identity theft involved the following types of fraud:

Credit card fraud	15%
Bank fraud	8%
Phone or utilities fraud	13%

Employment-related fraud	25%
Government documents/benefits fraud	14%
Loan fraud	3%
Other	23%
Attempted identity theft	5%

For many victims, identity theft is about more than the loss of money. It is about the loss of security, independence and self-worth. Endless paperwork. Pleading with creditors. Fending off debt collectors. Never knowing when, or if, it will stop.

3. HOW DO THIEVES GET PERSONAL OR FINANCIAL INFORMATION?

Personal identifying and financial information about you is available from many sources. Public records already contain information about birth dates, marriages, property ownership, and automobiles owned, just to name a few. Identity thieves look for even more private and personal information, including social security numbers, bank or credit card accounts, calling card accounts and other financial information. Here are just some of the ways they accomplish this:

- **Stealing your purse** or wallet to obtain social security cards, credit cards, drivers licenses, etc.
- **Stealing mail** being delivered to your home or left out for pick-up.
- **Diverting your mail** to another mailbox using a false "change-of-address" request.
- **"Dumpster diving"** -- thieves dig through dumpsters or garbage cans behind homes or businesses looking for discarded checks or bank statements, credit card or other account bills, medical records, pre-approved credit applications, etc.
- **"Shoulder surfing"** -- thieves watch over your shoulder as you enter your PIN into an ATM or as you key your long-distance calling card number into a pay telephone.
- **"Pretext calls"** -- thieves call to "verify" account information or to "confirm" an enrollment or subscription by having you repeat bank or credit card account numbers.
- **Using false or misleading Internet sites** to collect personal and financial information.
- **Burglarizing homes** looking for purses, wallets, files containing personal and financial information.
- **Computer hackers** "breaking into" business or personal computers to steal private client files and personal financial information.
- **Phony e-mail or "pop-up" messages** that appear to be from your credit card company, Internet Service Provider or other entity you do business with. These phony messages claim some problem with your account and direct you to another web site where you will be asked to supply credit card and other personal information.

4. WHAT ARE SOME TIPS ON PREVENTING ID THEFT?

- Be very cautious about giving your personal or financial information to anyone.
- **Never** provide personal identifying or financial information over the telephone when you did not initiate the call. Banks, credit card companies, telephone companies and other legitimate creditors do not call to "verify" account numbers or to ask for your social security number or other personal information.

- **Never** provide personal identifying or financial information over the telephone to anyone claiming to represent a contest or sweepstakes promotion.
- **Never** carry your social security card in your purse or wallet.
- **Never** have your social security number printed on your checks, drivers license or other financial documents.
- Purchase a simple "cross-cut" shredder (the kind that creates confetti, not the long strips) and get in the habit of shredding all personal or financial documents before placing them in the trash.
- Place password protection on all credit card accounts that allow it. Do not use common numbers or personal information (like birth dates or part of your social security number) or commonly chosen words (such as a child's, spouse's, or pet's name) for passwords.
- Control access to your credit history. Remove your name from mailing lists for pre-approved lines of credit by participating in the credit bureaus' "Opt-Out" program. Call 1-888-5-"OPT OUT" (1-888-567-8688) to enroll.
- **Never** leave outgoing mail in an unsecured mailbox overnight. If you are planning on being away from home on vacation, arrange with your post office to hold your mail.
- Take all credit card or ATM receipts with you after you pay for goods or services. Do not just leave them behind or throw them away in the nearest trashcan.
- Write to your bank, insurance company and other financial institutions you do business with and tell them not to share your customer information with unaffiliated third parties. Under federal law, they are required to honor this request.
- Remove your name from national direct mail advertising lists. To do this, send your name and address with a written request to: DMA Mail Preference Service, ATTN: Dept. 12059580, Direct Marketing Association, P.O. Box 282, Carmel, NY 10512.
- To dramatically reduce telephone solicitations, sign up with the Colorado No-Call List. You can register on-line at www.coloradonocall.com or by calling 1-800-309-7041.
- You can participate in the national no-call registry by going on-line at www.DONOTCALL.gov or by calling toll-free at 1-888-382-1222 (TTY: 1-866-290-4236).

5. WHAT SHOULD I DO IF I BECOME A VICTIM OF IDENTITY THEFT?

Start by contacting the fraud department of each of the three major credit bureaus to report the identity theft and request that the credit bureaus place a fraud alert and a victim's statement in your file. The fraud alert puts creditors on notice that you have been the victim of fraud, and the victim's statement asks them not to open additional accounts without first contacting you. Also, you may request a free copy of your credit report. Credit bureaus must provide a free copy of your report, if you have reason to believe the report is inaccurate because of fraud and you submit a request in writing.

The following are the telephone numbers for the fraud departments of the three national credit bureaus:
Trans Union: 1-800-680-7289;
Equifax: 1-800-525-6285;
Experian: 1-888-397-3742.

You should review your report to make sure no additional fraudulent accounts have been opened in your name, or unauthorized changes made to your existing accounts. Also, check the section of

your report that lists “inquiries” and request that any inquiries from companies that opened the fraudulent accounts be removed.

Next, contact any bank or other creditor where you have an account that you think may be the subject of identity theft. Advise them of the identity theft. Request that they restrict access to your account, change your account password, or close your account, if there is evidence that your account has been the target of criminal activity. If your bank closes your account, ask them to issue you a new credit card, ATM card, debit card, or checks, as appropriate.

In addition, you should file a report with your local police department and contact the FTC’s Identity Theft Hotline toll-free at 1-877-ID-THEFT (438-4338). The FTC puts the information into a secure consumer fraud database and shares it with local, state, and federal law enforcement agencies.

6. TIPS FOR MILITARY MEMBERS

If you are deployed away from your usual duty station and do not expect to seek new credit while you are deployed, consider placing an “active duty alert” on your credit report. An active duty alert requires creditors to take steps to verify your identity before granting credit in your name. An active duty alert is effective for one year, unless you ask for it to be removed sooner. If your deployment lasts longer than a year, you may place another alert on your report.

To place an active duty alert, or to have it removed, call the toll-free fraud number of one of the three nationwide consumer reporting companies. The company you call is required to contact the other two.

HELPFUL WEBSITES

ftc.gov/idtheft

https://aflegalassistance.law.af.mil

http://www.justice.gov/criminal/fraud/websites/idtheft.html