Identity Theft

You are sitting at home one evening, enjoying a nice dinner with your family when the phone rings and a debt collector informs you that you owe over $200 on a cellular phone account that you never opened. Before grabbing lunch at the PX, you realize you are low on cash and stop by the ATM only to find that your account is empty. You finally find your dream home, apply for a loan and start imagining how you will furnish and decorate your house when the bank calls to tell you that your credit is too poor to qualify for a loan.

Even if you have never experienced a similar scenario, you probably know someone who has. Since the 1990s, identity theft has become rampant through the United States, affecting almost 10 million victims in 2008 alone; therefore, it is important to know what steps to take both to protect yourself from becoming a victim and to respond if you do become a victim.

Unfortunately, thieves have a variety of options for stealing your identity. An identity thief might go through your wallet, garbage, or your mail for personal information. A more clever thief might steal records from your employer, buy personal information from sources inside your company, or send you a text or email posing as a bank or online service, requesting that you "verify your account information." Other common methods of identity theft include calling and pretending to be a legitimate business or government official who needs your information, posing as a landlord or employer to gain access to your credit reports. Hackers can get into an organization's computer and access all its data and can use spyware to see information on your personal computer.

Because potential identity thieves have so many different ways to gain access to your information, you have to protect yourself in several different ways. Many of the steps below seem obvious, but in the midst of a busy day, it is easy to forget the risks and opt for a short-cut that exposes you to identity theft. Though this list is not exhaustive, following the advice will make the identity thief's job much more difficult.

- Keep your confidential information private. If someone calls or emails you claiming to need your personal information, do not respond unless you are completely certain that the request is legitimate. Banks and credit card companies already have your confidential information.
- Monitor your bank and credit card transactions for unauthorized use.
- Write "see ID" on the back of each credit card.
- Order and review your credit report to make sure there is no erroneous information. You are allowed one free credit report from each agency every year. Their contact information is below.
- Secure your personal information, including financial documents, in your home.
- Shred your bills and other financial information.
- Memorize your PINs and passwords; do not write them down.
- Do not store credit card numbers and other financial information on your cell phone. Cell phones may be lost or stolen.
- Do not keep your social security card with you.
- When traveling, make sure to keep track of your credit cards and debit cards.

- If someone asks you for your social security number, ask why. Legitimate reasons include performing a credit check and reporting wages and taxes. Record-keeping is not a legitimate purpose.
- Remove your mail from your mailbox as soon as possible. Remember to put a vacation hold on your mail if you are going away. Go to www.usps.gov for more information on mail holds.
- Use only ATMs with monitoring cameras and be careful of people standing nearby who might be able to see you enter your PIN. Keep an eye out for suspicious devices on the ATM machine.
- Do not share sensitive information on social networking sites.
- Install antivirus software, antispyware, and firewall protections on your computer.
- Keep software up-to-date.
- Do not open emails from strangers. Do not open attachments unless you know the sender and know the contents of the attachment.
- Do not send confidential information via email.
- Do not click on pop-ups. Enable the pop-up blocker on your internet browser.
- Make online credit card purchases only from websites you trust.
- Do not keep financial and other sensitive information on your hard drive.
- Use strong passwords; avoid using anything that an outsider might guess, such as your child's name, your birthday, the name of your street, etc. And avoid using the automatic login feature that saves your username and password. Make sure to log off when you are finished.
- Be wary of online tax filing programs.

Even if you take all these steps to protect yourself, a creative thief might still find a way to steal your identity. Once stolen, the thief can use your personal information in many different ways, some of which are harder to detect than others. For example, if you monitor your bank account regularly, you will quickly detect if someone goes on a spending spree with your credit or debit cards; however, if someone uses your identity to open a new credit card account or bank account, take out loans, or establish household utilities, you will probably not detect it until much later. Some signs of such unauthorized accounts include: receiving credit cards for which you did not apply, denial of credit for no reason, and calls from debt collectors concerning debt you do not owe. If someone steals your social security number to get a job, you will likely not discover the fraud until tax-time when you do not receive your rebate. Thus, if you see warning signs that someone has stolen your identity to commit one type of crime, you should check to make sure that your identity is not being used for other purposes as well.

There are some general guidelines you should follow if you suspect that you are a victim of identity theft. First, make sure to document all of your correspondence, using certified mail, return receipt requested. Next, get copies of all the paperwork that credit bureaus, banks, credit card companies, and other businesses can provide concerning the suspected theft and its impact on your credit —make sure to keep the originals.

Once you determine that you have become a victim of identity theft, you should immediately take several steps to prevent the continued use of your information, protect your finances, and resolve any problems that might have occurred. While these steps may seem daunting and time consuming, to prevent as much damage as possible it is important to deal with the problem immediately and completely.

1. Contact the fraud department of one of the three major credit bureaus (see below for contact information).
   - Tell them that you are a victim of identity theft and request that a seven year fraud alert be placed on your file. The alert will be good for only 90 days unless you request that it remain for seven years.
   - Request that your file include a victim's statement asking that creditors call you before opening new accounts or changing existing accounts.
   - Request that inquiries from companies that opened fraudulent accounts be removed. Order copies of your credit report and review them to ensure no additional accounts have been opened or changes made. In addition to the free annual report, you are entitled to a free copy of your credit report if it is inaccurate due to fraud.
   - To place the initial fraud alert, you have to call only one of the three credit bureaus. As soon as one bureau confirms the alert, it will notify the other two.
   - You should continue to monitor your credit reports every three months to make sure that the changes have been made and that no new suspicious activity has occurred. After the initial fraud report, you will have to contact each of the three agencies on your own to order new reports.
2. Close unauthorized credit accounts that were opened fraudulently or accessed without authorization. Credit accounts are accounts with banks, credit card companies and other lenders, phone companies, utilities, internet service providers, etc.
   - Request that any unauthorized accounts or accounts the thief has accessed be processed as "account closed at consumer's request."
   - For new, unauthorized accounts, ask the company if it accepts the FTC's ID Theft Affidavit (available on the FTC's website at www.ft.gov/bcp/conline/pubs/credit/affidavit.pdf). The affidavit allows companies to investigate the fraud and decide your claim. If the company does not accept the affidavit, ask the representative to send you that company's fraud dispute form.
   - For existing accounts, ask the company for its fraud dispute form or write a letter explaining the situation. Make sure to get new account numbers and cards for compromised accounts.
3. Contact all creditors who have requested your credit report but not yet opened accounts and tell them not to open any accounts.
4. Cancel your ATM card, and get a new one with a new PIN.
5. Stop payment on checks that were stolen or misused, and notify your bank immediately if check fraud has occurred. In most states, the bank is responsible for losses from forged checks, if notified in a timely manner that the fraud has occurred. Ask the bank to notify the check verification company with which it does business.
   - To find out if someone is passing bad checks in your name, call 1-800-262-7771
   - Contact the major check verification companies and request that they notify any businesses that use their databases not to accept your checks.
     - TeleCheck: 1-800-710-9898
     - Certegy, Inc: 1-800-437-5120
     - International Check Services: 800-631-9656
6. File a police report with the local police or the police in the jurisdiction where the theft took place. Make a record of the report number and get a copy of the report, if possible. If you find out about new, unauthorized accounts or additional fraudulent activity, file new reports. Provide as much documentation (credit reports, ID Theft Affidavit, debt collection letters, etc.) as you can to the

police. A police report can help provide proof of the crime to banks, credit companies or other relevant businesses.

7. File a complaint with the FTC. For more information, go to the website at www.consumer.gov/idtheft or call 1-877-438-4338.
8. If you think someone is using your social security number to apply for jobs or get credit, contact the Social Security Administration at 1-800-772-1213 to verify the accuracy of your reported earnings and your name. You can also contact the Internal Revenue Service at 1-800-908-4490 to make sure that no one is using your social security number for employment.
9. If you think your driver's license is being used, contact your state department of registry of motor vehicles.
10. In some states, you can file a report with the state Attorney General.
11. If a debt collector contacts you about a debt you believe you do not owe, you have the right to dispute the debt. You must make the dispute in writing, within 30 days of the collector's initial contact.

Remember, you can always contact the Legal Assistance Office (533-3240) for additional help.

Credit Bureau contact information:
Equifax: www.equifax.com
- To order your report, call 1-800-685-1111
- To report fraud, call 1-800-525-6285 / TDD 1-800-255-0056
- P.O. Box 740241, Atlanta, GA 30374-0241

Experian: www.experian.com
- To order your report or to report fraud, call 1-888-397-3742 / TDD 1-800-972-0322
- P.O. Box 9532, Allen, TX 75013

TransUnion: www.transunion.com
- To order your report, call 1-800-888-4213
- To report fraud, call 1-800-680-7289 / TDD 1-877-553-7803
- Fraud Victim Assistance Department, P.O. Box 6790, Fullterton, CA 92834-6790

Other useful contacts:
- For information on identity theft in Hawaii, go to idtheft.hawaii.gov
- Department of Commerce and Consumer Affairs (DCCA) Resource Center for ID Theft Hotline: 1-808-587-3222
- FTC: www.consumer.gov/idtheft
- Social Security Administration: 1-800-772-1213
- Internal Revenue Service: 1-800-908-4490