PROTECTING AGAINST IDENTITY THEFT

How Can I Prevent Identity Theft from Happening to Me?

- As with any crime, you can't guarantee that you will never be a victim, but you can minimize your risk. By managing your personal information widely, cautiously and with an awareness of the issue, you can help guard against identity theft.
- Don't give out personal information on the phone, through the mail or over the internet unless you've initiated the contact or are sure you know who you're dealing with.
- Don't carry your SSN card; leave it in a secure place.
- Secure personal information in your home.
- Guard your mail & trash from theft.
- Carry only the identification information and the number of credit & debit cards that you'll actually need. Place passwords on your credit card, bank and phone accounts.
- Ask about information security procedures in your workplace or at businesses, doctor's offices or other institutions that collect personally identifying information from you.
- Give your SSN only when absolutely necessary.
- Pay attention to your billing cycles.
- Be wary of promotional scams.
- Keep your purse or wallet in a safe place at work.
- Cancel all unused credit accounts.

- When ordering new checks, pick them up at the bank rather than having them sent to your home mailbox.

- What should I do if someone has stolen or scammed my personal information or identification documents?

- If your information or identification documents were stolen or scammed, you have an opportunity to prevent the misuse of that information if you can take action quickly:

- For financial account information such as credit card or bank account information: Close those accounts immediately.

- For SSNs: Call the toll-free fraud number of any one of the three major credit bureaus and place a fraud alert on your credit reports.

- To replace an SSN card: Call the Social Security Administration at 1-800-772-1213 to get a replacement.

- For driver's license or other identification documents: Contact the issuing agency. Follow their procedures to place fraud flags and get replacements.

If you have a computer:

- Update your virus protection software regularly, or whenever a new virus alert is announced.

- Do not download files sent to you by strangers or click on hyperlinks from people you don't know.

- Use a firewall program, especially if you use a high-speed internet connection like cable, DSL or T-1 which leaves your computer connected to the internet 24-hours a day.

- Use a secure browser.

- Try not to store financial information on your laptop unless absolutely necessary.

- Look for website privacy policies.

- Before you dispose of a computer, delete personal information.