Identity Protection

Here are some times to keep your identity protected:

1. The next time you order checks, have only your initials (instead of first name) and last name put on them. If someone takes your checkbook, they will not know if you sign your checks with just your initials or your first name, but your bank will know!

2. Do not sign the back of your credit cards. Instead, write 'Photo ID Required'. Not all salespeople will look and ask, so if they do, thank them.

3. When you are writing checks to pay on your credit card accounts, DO NOT put the complete account number on the 'For' line. Instead, just put the last four numbers. The credit card company knows the rest of the number and anyone who might be handling your check as it passes through all of the check processing channels won't have access to it, or if it is stolen in postal transit.

4. Put your work telephone number on your checks instead of your home phone (if reasonable). If you have a PO Box, use that instead of your physical home address. NEVER have your social security number printed on your checks.

5. Photocopy all contents of your wallet. Do both sides of each license, credit card, etc. You will know what you had in your wallet as well as all of the account numbers and emergency call numbers in order to report the loss/theft. Keep the photocopy in a safe place. Also, carry an extra photocopy of your passport when you travel, either here or abroad.

When Something Is Lost/Stolen

We know we should cancel cards immediately – the key is having all of the toll free numbers and card numbers handy so you know whom to call.

File a police report immediately in the jurisdiction where your credit cards, etc., were stolen. This proves to credit providers that you were diligent, and this is a first step toward an investigation (if there ever is one).

Call the three national credit reporting organizations immediately to place a fraud alert on your name and social security number. The alert means any company that checks your credit knows your information was stolen, and they have to contact you by phone to authorize new credit.

Social Security Administration Fraud Line 800-269-0271

Protecting Your Personal Information

- Telephone Do's
  - Sign up with the national 'do not call' registry
  - Protect your calling card from prying eyes when out in public
  - Check your bill
- Telephone Don'ts
  - Give out your SSN or other personal data to calls you RECEIVE
  - List your phone number on your checks
  - Conduct personal business where you can be overheard

- ATM/Debit Card Do's
  - Use a PIN that is difficult to figure out
  - Watch for people looking over your shoulder
- ATM/Debit Card Don'ts
  - Use convenience store ATMs – they may not be as secure as bank machines
  - Use your debit card for online shopping or pay at the pump gas stations; use a credit card. Debit cards give access directly to your bank account; credit cards often have better protection for problems with merchandise.

- Computer Do's
  - Use up-to-date virus and security protection
  - Use one credit card for internet shopping
  - Clean the hard drive of computers you discard
  - Close your browser after online banking or shopping
- Computer Don'ts
  - Store personal information or passwords on your computer
  - Store credit or bank card numbers on your computer
  - Open or respond to unknown email, especially attachments
  - Fall for 'phishers' – scammers who send legitimate-looking emails trying to get your personal information.

- US Mail Do's
  - Use a secure mailbox for your outgoing mail
  - Check your statements and bills every month
  - Shred anything containing personal information
  - Reduce the amount of solicitations you receive
- US Mail Don'ts
  - Have checks, blank or otherwise, sent to an unlocked mailbox