

PREVENTATIVE MEASURES

Your greatest asset for securing your good name is in understanding where the thieves get your information. Here are a few of the many ways thieves can obtain your personal identifying information:

- Coming into possession of your lost or stolen wallet or purse.
- Stealing your mail, or diverting it to another mailbox via a change of address request.
- "Dumpster Diving" into your trash and gathering important documents.
- "Pretext" calls where the thief poses as your bank, internet service provider, or other organization with which you may or may not have had financial dealing and they call you to "verify your account information" because of a problem they had with their "records system."
- Other crimes such as burglary or breaking into a vehicle where the thief looks to steal financial information, wallets, purses, or other items containing such information.
- Internet transactions on unsecured sites or with illegitimate companies posing as a reputable "safe" business with which you may do business.

Knowing how the thieves get the information, it is now clear how best to protect that information: you should begin immediately to practice these simple steps:

1. Protect your Social Security number, credit card numbers, account passwords and other personal information.

Use common sense, and be suspicious when things don't seem right. Never divulge your information over the phone unless you initiated the phone call. If personal information is requested ask questions. It is your right to know why it's needed, how it will be used, and who needs it.

If you get an unsolicited offer that **sounds too good to be true, it probably is!** If a caller claims to represent your financial institution, the police department or some similar organization and asks you to "verify" (reveal) confidential information, hang up fast and consider reporting the incident. Real bankers and government investigators don't make these kinds of calls.

2. Minimize the damage in case your wallet gets lost or stolen.

Don't carry around more checks, credit cards or other bank items than you really need. Limit the number of credit cards you carry by canceling the ones you don't use. Don't carry your Social Security number in your wallet or have it pre-printed on your checks. Pick passwords and Personal Identification (PIN) numbers that will be tough for someone else to figure out – don't use your birth date or home address, for example. Don't keep this information on or near your checkbook, ATM card or debit cards. Also, don't leave your wallet unattended in a store, restaurant, office or other public place even for a few minutes.

3. Protect your incoming and outgoing mail.

Promptly remove mail from your mailbox after it has been delivered. If you're going on vacation have your mail held at your local post office or ask someone you know and trust to collect your mail. Deposit outgoing mail in the Postal Service's blue collection boxes, hand it directly to a mail carrier, or take it to a local post office.

When writing checks use "gel-ink" pens. Checks written using "gel" ink are currently more difficult to 'wash' (chemically erase) and therefore more difficult to forge or counterfeit.

4. Keep thieves from turning your trash into their cash.

"Dumpster divers" pick through trash looking for pre-approved credit card applications and receipts, canceled checks, bank statements, expired charge cards and other documents or information they can use to counterfeit or order new checks or credit cards. To keep this from happening, use a "cross-cut" shredder and shred any document that contains any part of or all of your personal information. "Cross-cut" shredding makes confetti out of the documents and makes it virtually impossible for the thief to paste them back together.

5. Practice home security.

Safely store extra checks, credit cards, or other financial documents. Consider using a document safe for these items. Don't advertise to burglars that you're away from home. Use timers on your lights and temporarily stop delivery of your newspaper and mail or ask a trusted neighbor to pick up any items that may arrive unexpectedly at your home.

6. Pay attention to your bank account statements and credit card bills.

ALWAYS check into discrepancies in your records or if you notice something suspicious, such as a missing payment or an unauthorized withdrawal. Also, contact the appropriate institution if a bank statement or credit card bill doesn't arrive on time because that could be a sign someone has stolen account information and changed your mailing address in order to run up big bills in your name from another location.

7. Review your credit report approximately once a year.

Monitor your credit report for accuracy, looking for unauthorized bank accounts, credit cards, purchases, etc. Look for anything suspicious in the section of your credit report that lists who has received a copy of your credit history. This may be an indication a thief is trying to obtain fraudulent benefits, or is merely casing you as a viable victim.

To order your report, call the three major credit bureaus at these toll-free numbers: Equifax at (800) 685-1111, Experian at (888) 397-3742, or Trans Union at (800) 888-4213. By law, the most you can be charged for a copy of your report is \$8.50. To be safe, consider getting a copy from each of the three companies.

8. Practice "on-line" or internet safety.

Be suspicious of web offers that seem too good to be true. Ensure the web site you are using is legitimate, or has been formally examined and certified secure and reliable by a legitimate certifying agency such as the Better Business Bureau.

Use your credit card and social security number only when absolutely necessary. Only use websites you believe are using secure communication links that are encrypted (scrambled). Look for the small golden 'lock' icon at the bottom right of the screen if using Microsoft Internet Explorer, or the URL designation 'https:' where the 's' indicates that you are communicating via an 'encrypted' and therefore more secure connection. Again, keep your PIN numbers and passwords confidential, and DON'T write them down and leave them next to, on or near your computer.