IDENTITY THEFT Protect Your Personal Information

How do thieves get your information?

They get information from businesses or other institutions by:

- Stealing records or information while they're on the job
- Bribing an employee who has access to these records
- Hacking those records
- Conning information out of employees
- Sometimes thieves get information due to you or someone else being careless and unaware of the importance of guarding your personal information!

Other ways thieves may get your information:

- Steal your wallet or purse.
- Steal personal information they find in your home.
- Steal your mail, including bank and credit card statements, credit card offers, new checks, and tax information.
- Get your credit reports by abusing their employer's authorized access to them, or by posing as a landlord, employer, or someone else who may have a legal right to access your report.
- Rummaging through your trash, the trash of businesses, or public trash dumps in a practice known as "dumpster diving."
- Swiping your card for an actual purchase, or attach a skimming device to an ATM where you may enter or swipe your card.
- Completing a "change of address form" to divert your mail.
- Stealing your credit or debit card numbers by capturing the information in a data storage device in a practice known as "skimming."
- Stealing personal information from you through email or phone by posing as legitimate companies and claiming that you have a problem with your account. This practice is known as "phishing" online, or pretexting by phone.
- Calling your credit card issuer to change the billing address on your credit card account. The imposter then runs up charges on your account. Because your bills are being sent to a different address, it may be awhile before you realize there's a problem.

Thieves use your personal information by:

- Opening new credit card accounts in your name. When they use the credit cards they don't pay the bills, the delinquent accounts are reported on your credit report.
- Getting a job or filing fraudulent tax returns in your name.
- Establishing phone or wireless service in your name.
- Opening bank accounts in your name and then write bad checks on that account.
- Make counterfeit checks or credit or debit cards, or authorizing electronic transfers in your name, and drain your bank account.
- Filing for bankruptcy under your name to avoid paying debts they've incurred under your name, or to avoid eviction.
- Getting identification such as a driver's license issued with their picture, in your name.
- Giving your name to the police during an arrest. If they don't show up for their court date, a warrant for arrest is issued in your name.

Steps you can take to avoid becoming a victim:

- Don't keep your social security card in your wallet.
- Never provide your personal information to anyone who contacts you through a phone solicitation.
- Check your bills and bank statements as soon as they arrive.
- Opt out of pre-approved credit offers. Call 1-888-5OPT-OUT or visit OptOutPrescreen.com to be removed from pre-approved credit lists.
- Check your credit reports often by contacting the major three credit reporting agencies: Equifax 800-525-6285; Experian 888-397-3742; TransUnion 800-680-7289
- Don't list your birthday and/or social security number on resumes.
- Use your ATM card wisely.
- Guard your checkbook
- Secure personal information in your own home.
- Shred personal information with a crosscut type shredder
- Get all of your checks delivered to your bank - not your home address.
- Put passwords on all your accounts and do not use your mother's maiden name. Make up a fictitious word and use numbers and symbols.
- Do not put your credit card account number on the Internet (unless it is encrypted on a secured site.)
- Don't put account numbers on the outside of envelopes, or on checks.
- Do not put checks in the mail from your home mailbox. Drop them off at a U.S. Mailbox or the U.S. Post Office. Mail theft is common. It's easy to change the name of the recipient on the check with an acid wash.
- Make a list of all your credit card account numbers and bank account numbers (or photocopy) with customer service phone numbers, and keep it in a safe place. (Do not keep it on the hard drive of your computer if you are connected to the Internet.)

What to do if your identity is stolen:

- Immediately report lost or stolen credit cards and debit cards.
- Close accounts that you know, or believe have been tampered with or opened fraudulently.
- File a report with your local police or the police in the community where the identity theft took place.
- Place a fraud alert on your credit reports, and review them often.

Contact

Financial Crimes Unit • 315 Fourth Avenue, Chula Vista, CA 91910 • **www.chulavistapd.org** • **(619) 691-5187**