

Identity Theft Prevention and Recovery

Prevention

Everyday

- Don't give out personal information on the phone, through mail, on the Internet or even in person, unless you've initiated the contact or you are sure the caller/company is legitimate.

- Keep your personal information like your ATM pin number, social security card, birth certificate, etc. in a secure location, even at home. This is especially important if you have roommates, a cleaning service or are having house work done at home.

- Do not leave your Social Security Card in your wallet.

- Before throwing away documents with personal information, make sure to shred, cut, or mark out your personal data.

- Keep an eye on your purse or wallet; report it to the police and credit card companies immediately.

- Deposit outgoing mail in a secured mailbox

- Promptly remove your mail from an unsecured mailbox. If you are leaving on vacation n request a hold from the Postal Service.

- Use a firewall program with your high speed Internet connection to stop uninvited access to your computer

- Only use secure sites to provide personal or financial information through an organization's website

- Only provide your SSN when absolutely necessary and ask to use other types of identifiers

Regularly

- Monitor the balances of your financial accounts. Look for unexplained charges or withdrawals.

- Review your credit report to make sure new credit card accounts have not been opened in your name

- Regularly update virus protection software on your computer

- Try not to store financial information on your laptop

- If you need to provide personal or financial information online look for a lock icon on the browser status bar or a URL that begins with https.

- Be

conscious of unreceived bills or mail. If you do not receive your monthly bills, checks, etc... it may mean someone submitted a change of address for you.

- Place passwords on your credit card, bank and phone accounts. Avoid using easily available information like your date of birth, mother's maiden name, etc...

- When opening a new account with an application that asks for your mother's maiden name, ask to use a password instead.

- Ask about information security at your workplace or businesses that collect your personal information (banks, doctors' offices, schools etc.). Find out how it is disposed, who it shared with and how it can be kept confidential.

- Before disposing of a computer, delete all the personal information it stored with a "wipe" utility program to overwrite the entire hard drive.

Never

- Do not open files or links emailed to you from a person or company you don't know

- Don't use an automatic log-in feature that saves your user name and password and always log off when you're finished

- When ordering new checks, pick them up at your bank do not have them mailed to you.

Actions to take if you may be a victim

It is important to act quickly in the following ways to prevent or halt any damage that may have occurred. Make sure to keep a record of all correspondence concerning the matter.

- Report a stolen wallet, credit cards or identification documents immediately to the local police.

- Place a fraud alert on your credit reports and review your credit report

- Call one of the following companies to place an alert on your report. They are legally required to contact the other two.

Equifax

1-800-525-6285

<http://www.equifax.com/>

P.O. Box 740224 Atlanta, CA 30374

Experian

1-888-397-3742

<http://www.experian.com/>

P.O. Box 9532

Allen, TX 75013

TransUnion

1-800-680-7289

<http://www.transunion.com/>

P.O. Box 6790

Fullerton, CA 92834