

Identity Theft: Don't Be A Victim

Prevention Checklist

- Wear a close-fitting pouch or carry a wallet in your front pocket instead of carrying a purse.
- Don't carry your checkbook, debit card or excess credit cards in public.
- Copy the contents of your wallet.
- Remove everything from your wallet containing your SSN, including your Social Security card, Medicare card, military ID card. If your SSN is on your Driver's License – get a new license.
- Don't give any part of your Social Security, credit card or bank account numbers over the phone, e-mail or Internet, unless you have initiated the contact to a verifiable company or financial institution.
- Request a free copy of your credit report once a year: **Equifax, 800-685-1111, www.equifax.com**, P.O. Box 740241, Atlanta, GA 30374-0241; **Experian, 1-888-397-3742, www.experian.com**, P.O. Box 2002, Allen TX 75013; **Trans Union, 1-800-888-4213, www.transunion.com**, P.O. Box 1000, Chester, PA 19022
- Notify the credit reporting agencies of the death of a relative or friend to block the misuse of the deceased person's credit.
- Call your bank and credit card customer service and ask to "opt out" of ALL marketing programs, including 'convenience' checks mailings.
- Call **1-888-567-8688** to "opt out" of credit agency marketing lists and reduce credit card solicitations.
- Shred pre-approved credit card offers, and all financial documents, preferably with a crosscut shredder.
- Mail bills to be paid inside the Post Office, or use automated payment plans or online banking.
- Ask your bank or credit union to send boxes of new checks to them for you to pick up, not to your home.
- Check your earnings record at least annually and more often if you suspect your SSN has been compromised (it's free and there is no limit to how often you may request it.) Call the Social Security Administration at **1-800-772-1213** and ask for Form SSA-7004, *Request for Earnings and Benefit Estimate Statement*. The *Statement* will show the earnings reported to your SSN each year since 1951. You may request the form online at: <http://www.ssa.gov/mystatement/>

Computer Precautions

- Never respond to e-mails requesting personal information such as account and Social Security numbers or passwords, even if the sender appears to be your bank, the Federal Deposit Insurance Corporation, Social Security Administration, IRS, AOL, eBay, PayPal, etc. No legitimate company or agency will send an e-mail asking you to verify personal information.
- Delete unknown or questionable e-mails without opening.
- Use a firewall program, especially if you use a high-speed connection like cable, DSL or T-1, which connects your computer 24 hours a day.
- Use a secure browser - software that encrypts or scrambles information you send over the Internet - to guard the security of online transactions.

What To Do IF Your Identity is Stolen

Resolving the consequences of identity theft is left largely to the victims. It's important to act quickly and assertively to minimize the damage.

File a report with your police, sheriff or district attorney and get a copy of the report for the credit agencies, banks and credit card companies.

Cancel each credit card. If you report the loss before the cards are used, you are not responsible for any unauthorized charges. Beware of callers selling credit card protection – you don't need this! Carefully monitor your credit card statements for evidence of fraudulent activity.

Contact your financial institution and cancel all accounts and PIN numbers. Stop payments on outstanding checks and complete "affidavits of forgery" on unauthorized checks.

Report the theft to the fraud units of the three credit reporting agencies: **Equifax 1-800-525-6285; Experian 1-888-397-3742; Trans Union 1-800-680-7289**. Request the credit reporting agencies flag your credit file for fraud, and add a victim's statement to your report, such as "My identification has been used to apply for fraudulent credit. Contact me at (your telephone number or address) to verify ALL applications."

Ask utility companies (especially cellular service) to watch for anyone ordering services in your name. If you have trouble with falsified accounts, contact the Public Utility Commission.

You are not responsible for ID theft losses. Don't be coerced into paying a fraudulent debt.

Resources:

State of Colorado	http://www.ago.state.co.us/idtheft/welcome.htm
Denver District Attorney	720-913-9196 or 720-913-9179
Jefferson County District Attorney	303-271-6931
Arapahoe/Douglas County District	720-874-8506
Adams County District Attorney	303-654-6227
Federal Trade Commission	1-877-438-4338 http://www.consumer.gov/idtheft

Identity Theft: Don't Be A Victim: produced by:

The Denver District Attorney's Office
Call 720-913-9196 or 720-913-9179
for personal assistance - www.denverda.org

Qwest

www.qwest.com/identitytheft

800-244-1111

The Colorado Bankers Association

TransUnion