



## ID THEFT PREVENTION:



1. Buy a cross-cut type shredder (you can purchase cross-cut type shredder very cost effectively for approximately \$60 - \$70.) Shred all your important papers and especially pre-approved credit applications received in your name and other financial information that provides access to your private information. Don't forget to shred your credit card receipts.
2. Be careful of "Dumpster Diving." Make sure that you do not throw anything away that someone could use to become you. Anything with your identifiers must be shredded (cross-cut) before throwing away.
3. Be careful at ATM's and using Phone Cards. "Shoulder Surfers" can get your "Pin Number" and get access to your accounts.
4. Get all of your checks delivered to your bank - not to your home address.
5. 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.
6. When you order new credit cards in the mail, or your previous ones have expired, watch the calendar to make sure that you get the card within the appropriate time. If not received by a certain date, call the card grantor immediately and find out if the card was sent. Find out if a change of address was filed.
7. Cancel all credit cards that you do not use or have not used in 6 months. Thieves use these very easily - open credit is a prime target.
8. Put passwords on all your accounts and do not use your mother's maiden name. Make up a fictitious word.
9. Get a post office box or a locked mailbox, if you possibly can.
10. Ask all financial institutions, doctors' offices, etc., what they do with your private information and make sure that they shred it and protect your information. Tell them why.
11. Empty your wallet of all extra credit cards and social security numbers, etc. Do not carry any identifiers you do not need. Don't carry your birth certificate, social security card, or passport, unless necessary.
12. Memorize social security numbers and passwords.
13. When a person calls you at home or at work, and you do not know this person, never give out any of your personal information. If they tell you they are a credit grantor of yours call them back at the number that you know is the true number, and ask for that party to discuss personal information. Provide only information that you believe is absolutely necessary.
14. Do not put your social security number on your checks or your credit receipts. If a business requests your social security number, give them an alternate number and tell them why. They do not need that to identify you. If a government agency requests your social security number, there must be a privacy notice accompanying the request.
15. Do not put your telephone number on your checks.
16. Get credit cards and business cards with your picture on them.
17. 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 your checks.
18. When you are asked to identify yourself at schools, employers, or any other kind of institutional identification, ask to have an alternative to your social security number. Unfortunately, your health insurance carrier often uses your social security number as your identification number. Try to change that if you can.

19. In conjunction with a credit card sale do not put your address, telephone number, or driver's license number on the statement.

20. Monitor all your bank statements from every credit card every month. Check to see if there is anything that you do not recognize and call the credit grantor to verify that it is truly yours.

21. Order your credit report at least twice a year. Review it carefully. If you see anything that appears fraudulent, immediately put a fraud alert on your reports by calling the numbers below and immediately correct all mistakes in writing.

22. Take your name off all promotional lists. Call the three credit reporting agency numbers to opt out of pre-approved offers.

**Equifax:** 1-800-525-6285 ([www.equifax.com](http://www.equifax.com))

**Experian:** 1-888-397-3742 ([www.experian.com](http://www.experian.com))

**TransUnion:** 1-800-680-7289 ([www.transunion.com](http://www.transunion.com))

**Social Security Administration** (fraud line): 1-800-269-0271

Write to the following to get off promotional lists:

Direct Marketing Association  
Mail Preference Service  
P. O. Box 9008  
Farmingdale, NY 11735

Direct Marketing Association  
Telephone Preference Service  
P. O. Box 9014  
Farmingdale, NY 11735

**To get off pre-approved credit card mailings, call 1-888-5OPTOUT (1-888-567-8688) or [www.optoutprescreen.com](http://www.optoutprescreen.com).**

23. Consider making your phone an unlisted number or just use an initial.

24. 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.)

### **Contact Creditors and Financial Institutions**

If a credit card or banking account has been tampered with, you should immediately contact their security or fraud department and close the account. If you open a new account, select a new password or PIN, and change passwords on all unaffected accounts as well. Follow up any telephone call with a certified letter, especially when it pertains to a credit card account. **As of June 1, 2005, Oklahomans can check their credit report once a year at no charge. To do this online, go to [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1.877.322.8228.**

### **File a Report**

File a report with the local police department and keep a copy for your records.

\* Contact the Federal Trade Commission (FTC), which maintains the Identity Theft Data Clearinghouse and provides information to identity theft victims. You can call toll-free 1-877-ID-THEFT (1-877-438-4338), send mail to: Identity Theft Data Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, or you can file an ID Theft Affidavit online at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)

\* If your mail has been stolen, notify your local postal inspector at [www.usps.gov/websites/depart/inspect](http://www.usps.gov/websites/depart/inspect). Mail theft is a federal crime.

\* Notify the Social Security Administration if your Social Security Number has been misused. Call the SSA Fraud Hotline at 1-800-269-0271; fax: 410-597-0118; write: SSA Fraud Hotline, P.O. Box 17768, Baltimore, MD 21235; or e-mail: [oiq.hotline@ssa.gov](mailto:oiq.hotline@ssa.gov).

**Oklahoma Bankers Association**, PO Box 18246, OKC, OK 73154 405.424.5252  
**Fraud Unit** Elaine Dodd [elaine@oba.com](mailto:elaine@oba.com) Fraud Unit Sponsored by Deluxe Checks