



November 2004

**Minnesota Crime Prevention Association's
Tips of the Month**

IDENTITY THEFT

1. Purchase a cross shredder to shred all your personal documents.
2. Consider putting a fraud alert on your credit accounts. Contact the major credit bureaus to place a fraud alert on your credit file. Future creditors will then have to contact you to confirm any new accounts by phone.

Credit Reporting Agencies:

TransUnion LLC - <http://www.tuc.com>

To order your report, call 1-800-916-8800 or write:

Consumer Disclosure Center
P.O. Box 1000 Chester, PA 19022

To report fraud, call 1-800-680-7289 / TDD: 877-553-7803 or write:

Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92634

Equifax Information Services, LLC - <http://www.equifax.com>

To order your report, call 1-800-685-1111 or write:

P.O. Box 740241
Atlanta, GA 30374

To report fraud, call 1-800-525-6285 / TDD: 800-255-0056 or write:

P.O. Box 740241
Atlanta, GA 30374

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

To order your report, call 1-888 EXPERIAN (888-397-3742) or write:

P.O. Box 2104
Allen TX 75013

To report fraud, call 1-888 EXPERIAN (888-397-3742) or write:

P.O. Box 9532
Allen TX 75013

3. Slow the flow of junk mail and telemarketers which is mostly a waste of time and resources. About 62 million trees and 25 billion gallons of water are used to produce a typical year's worth of junk mail in the United States. Worst of all, it puts you at greater risk for identity theft because each pre-approved credit offer that's sent to you is another invitation for someone to open a credit line in your name. To remove your name from the marketing lists of the three credit reporting bureaus: **call the Opt-Out Line: 1-888 567-8688**

4. Be Aware of Scams

You've Won a Prize!" Scam

We all want to be winners but don't be fooled into giving out your personal information. If someone calls you to offer you the chance to receive a "major" credit card, a prize, or other valuable item, but asks you for personal data -- such as your Social Security Number (SSN), credit card number, expiration date, or mother's maiden name – be cautious! Ask them to send you a written application form. If they won't, tell them you're not interested and hang up. If they send it, review the application carefully and make sure it's going to a company or financial institution that's reputable.

Nigerian Scam

This scam has been used for over a decade and is sent out to victims via letter, e-mail, or fax. It consists of a message stating the sender has a large sum of money, usually \$10 million or more, and needs help transferring it out of Nigeria or some other country. As a reward for your help, the sender promises to pay you a percentage of the transferred funds. Don't give out your bank account number or any other personal information! The Better Business Bureau can give you information about businesses that have been the subject of complaints.

5. Protect Your Social Security Number

One of the most important things you can do to protect yourself from identity theft is to protect your Social Security Number. Your SSN is the key to your personal information. By obtaining it a thief can get access to many things including your bank accounts and Credit cards. Protect your Social Security Number:

- ? Do not carry your Social Security Card in your wallet or purse. Keep this card in a safe place at home.
- ? Do not imprint your SSN on your checks.
- ? When asked to provide your SSN, ask the individual why it is needed and how they will be using the number.
- ? Do not post your SSN in emails or chat rooms.
- ? When applying for something online make sure that the site is secure.
- ? Read the Privacy Policy of any website to which you may provide personal information. The policy will let you know how they use your information.

6. Reduce the amount of personal information that is "out there".

7. Sign up for the Federal Trade Commission's **National Do Not Call Registry** and the Direct Marketing Association's Telephone Preference Service. Your name is added to "deletion lists" used by nationwide marketers. You may also need to register for your state's "do not call" list.

National Do Not Call Registry, www.donotcall.gov, (888) 382-1222

Telephone Preference Service, PO Box 1559, Carmel, NY 10512

Do Not Call Registry interaction with state registries:

www.ftc.gov/bcp/online/edcams/donotcall/statelist.html

8. Have your name and address removed from the phone book and reverse directories.

(www.privacyrights.org/fs/fs4-junk.htm.)

9. Install a locked mailbox at your residence to deter mail theft or use a post office box or a commercial mailbox service. When you are away from home for an extended time, have your mail held at the Post Office or ask a trusted neighbor to pick it up.

10. Pick up new checks at the bank rather than have them mailed to your home. If you have a post office box, use that address on your checks rather than your home address so thieves will not know where you live.
11. When you pay bills, do not leave the envelope containing your check at your mailbox for the postal carrier to pick up, or in open boxes at your workplace. If stolen, your checks can be altered and then cashed by the imposter. It is best to mail bills and other sensitive items at the Post Office.
12. Reduce the number of credit cards you actively use to a minimum and carry only one or two in your wallet. Consider canceling unused accounts. Even though you do not use them, their account numbers are recorded in your credit report, providing a tempting target for identity thieves. Be aware that reducing the number of credit card accounts might lower your credit score. Part of your score is determined by having credit cards and installment loans and making timely payments. (For more information on credit scoring, visit www.myfico.com.)
13. Photocopy or keep a list of all your credit card, bank account, and investment account numbers. Make note of expiration dates and telephone numbers of the customer service and fraud departments. Keep these in a secure place (not your wallet or purse) so you can quickly contact these companies in the event your credit cards are stolen or accounts are used fraudulently.
14. Identity thieves have been known to call their victims with a fake story that goes something like this. "Today is your lucky day! You have been chosen by the Publishers Consolidated Sweepstakes to receive a free trip to the Bahamas. All we need is your Social Security Number, credit card number and expiration date to verify you as the lucky winner." **Never** give out your SSN, credit card number or other personal information over the phone, by mail or on the Internet unless you have a trusted business relationship with the company and you have initiated the call.
15. Always take credit card receipts with you. Never toss them in a public trash container. When shopping, put receipts in your wallet rather than in the shopping bag. Never permit your credit card number to be written onto your checks.
16. Watch the mail when you expect a new or reissued credit card to arrive. Contact the issuer if the card does not arrive promptly.
17. Order your credit report once a year, or better twice, from each of the three credit bureaus to check for errors and fraudulent use of your accounts. Credit reports cost \$8-\$9 in most states. If you are on a budget, order from one credit bureau now, from another in six months, and the third six months later. In one year you will have checked all three. For more information on credit reports log onto: www.privacyrights.org/fs/fs6-crdt.htm.

Resources from:

Minnesota Attorney Generals Office: www.ag.state.mn.us

Federal Trade Commission: www.consumer.gov/idtheft

U.S. Department Of Justice www.usdoj.gov/criminal/fraud/idtheft.html

U.S. FBI <http://norfolk.fbi.gov/1999/ident.htm>