IDENTITY THEFT PREVENTION

PROTECT YOUR SOCIAL SECURITY NUMBER; IT IS THE KEY TO YOUR IDENTITY.

- Do not carry anything with your or anyone's Social Security Number, birth certificate or passport in your wallet, purse or vehicle. If your Medical Card (Including Medi-Care/Medi-Cal), insurance or military card still has your SSN on it photocopy the card and black out the SSN, then carry the copy.

- Do not provide your SSN (or any part of it) in person, over the phone, or over the Internet, unless you are applying for credit or verifying your identity to an institution where you initiated the contact and know you are dealing with a legitimate company. Ask institutions to have a password (Not your SSN) for identity verification.

- If you must provide your SSN do not give it over a cell phone or cordless home phone. You never know who might be listening.

- If someone asks for your SSN ask why he/ she needs it, what they need it for, and how they will protect it. Ask your doctor, dentist, optometrist, tax preparer, school, bank, financial advisor, mortgage broker....anyone who has a legitimate reason to have your SSN, what they do to protect your information.

HOME SECURITY/VEHICLE SECURITY

- Lock any document with your SSN in a safe to keep it out of the hands of burglars, hired help, contractors, or not so nice family or friends. Their target is your identity.

- Invest in a confetti shredder and shred all financial documents, including bank statement, pre-approved credit card offers, receipts, and utility bills, before you throw them away.

- DO NOT put outgoing mail in your mailbox. Bring it to the Post Office.

- Unless you can retrieve your mail as soon as it is delivered, get a locking mailbox or P.O. Box for bills and financial documents.

- Do not keep anything with your personal information, including address, in your car. If you keep your registration in your car (vs. on your person) black out the address so an auto burglar doesn't obtain your address and garage door opener, then burglarize your home.

BANKING SECURITY/ FINANCIAL SECURITY

- DO NOT put your SSN, Driver's license number, or phone number on your checks. Consider putting only your first initial and last name.

- DO NOT put full account numbers in the memo section of check or on the outside of the return envelope.

- Have your checks sent to your bank branch NOT your home.

- Get an ATM card or revolving credit card only, not a Visa or MasterCard Check Card, which is attached to your bank account. If your check card number is compromised or skimmed, the money is removed directly from your account and while you are proving to your bank you did not make the purchases, your

legitimate checks are bouncing. If you must carry a check card, do not let it out of your sight, even at restaurants, because that gives the merchant the opportunity to "Skim" your information, which is then retained and reprogrammed onto a counterfeit credit card.

- Check your bills and bank statements right away. Check carefully for any unauthorized charges or withdrawals and report them immediately. If you do not catch them in time (Usually within 30-60 days) you might not be reimbursed by your bank and/or responsible for unauthorized charges to your credit card.

INTERNET SAFETY

- Shield your computer from viruses and spies. Use firewall and virus protection software that you update regularly. Download virus/firewall from sites you know and trust or purchase from a reputable merchant.
- Password protect your log-in.

- Do not click on links in pop-up windows or in spam email.

- When shopping online, only enter personal information on secure Web pages with "https" in the address bar and a padlock symbol at the bottom of the browser window. These are signs that your information will be encrypted or scrambled, protecting it from hackers.

- Fight "phishing". Scam artists "phish" for victims by pretending to be banks, stores or government agencies. They do this over the phone, in emails and in the regular mail. Don't give out your personal information- unless you made the contact. Don't respond to a request to verify your account number, password, or "Update" your information. Legitimate companies do not request this kind of information in this way.

- Educate your children about the dangers of providing personal information to anyone online.

ULTIMATE SECURITY

- Even if you take all of the above precautions your information could be compromised in a number of other ways you cannot prevent, so..

- Catch it quick by password protecting and monitoring your existing accounts and check your credit report with all three credit-reporting agencies at least 2 times a year. www.annualcreditreport.com provides one free credit report a year. (Obtaining your own credit report does not affect your credit score.)

- Obtain credit monitoring through your bank or another reputable source. A credit monitoring service, for a fee, notifies you if there are any changes to the credit reporting bureaus under your SSN, including inquiries, offers quarterly or unlimited credit reports, and often provides ID Theft insurance. Make sure you sign up for a service that monitors all three credit reporting bureaus, Equifax, Experian, and Transunion. Some reputable sources are Equifax "Credit Monitoring Gold 3 in 1", Costco "Identity Guard" and Wells Fargo "Select" Identity Theft Protection.

- Place a "Credit Freeze" on all three credit-reporting bureaus. Merchants typically will not approve credit if they cannot access your credit score. To place a credit freeze on your reports visit the California Office of Privacy Protection website at www.privacyprotection.ca.gov, click on "Identity Theft" then "How to "Freeze" Your Credit Files"