

DON'T become a victim of identity theft!

You can greatly minimize your chances by implementing the safeguards listed below:

- Be extremely cautious when handling and disclosing the following information:
 - Social Security Number
 - Mother's Maiden Name
 - Date of Birth
 - Current and Past Addresses
 - Drivers License Number
 - Bank Account Numbers
 - Credit Card Account Numbers
 - Personal Identification Number (PIN) Codes

Never provide personal information over the phone, unless you have initiated the phone call. If you receive a call and want to confirm that the company is who they say they are, ask for a call back number and match it against the telephone book or directory assistance. Check with the Better Business Bureau to determine the legitimacy of the business.

- Never leave outgoing checks or paid bills in your residential mailbox. Use a blue postal mailbox or your local post office.
 - Consider installing a residential mailbox that is equipped with a locking mechanism and never leave mail in your mailbox overnight.
- When ordering new checks, do not have them sent to your residence. Pick them up at the bank or have them delivered by registered mail.

- Use a shredder prior to disposing of bank and credit card statements, canceled checks, pre-approved credit card offers, and any other financial or personal information. A crosscut shredder offers added security by making it more difficult to reconstruct shredded documents.

- Place your garbage out in the morning on the day of pickup rather than the night before. "Dumpster divers" have less opportunity to go through your garbage.

- If you list your name in the telephone book consider leaving out your address, or having an unpublished number. Leave off titles such as "Dr." or "Attorney" or any other signs announcing your apparent affluence.

- Minimize the amount of information you carry in your wallet or purse by taking out extra credit cards and ID's.
- Cancel all unused credit cards and maintain a list of active cards and accounts.
 - This list should include account numbers, expiration dates, telephone numbers and addresses for each creditor. Store this information in a secure place.

- Open all bills promptly and check your accounts monthly.
 - Save all credit card receipts and match them against your monthly billing. Look for charges you don't recognize and report them immediately.



- Call your credit card company if your card has expired and you have not yet received a replacement.
- Notify your credit card companies and financial institutions in advance of any address or phone number changes.
- Never loan your credit cards to anyone.
- Sign all credit cards upon receipt.

- Report all lost or stolen credit cards immediately.
- Be cautious of "shoulder surfers." Always shield your calling card or pin numbers when entering them during a transaction.

- Keep your eyes on your credit card during all transactions (i.e. restaurants)
- Never leave transaction receipts behind including, ATM receipts on the counter, at the gas pump, at the bank, or in a trash receptacle - *these should be shredded.*
- Ask your creditors to include a security password on your accounts. Refrain from using your mother's maiden name.
- Limit the information printed on your checks to your name and address. If the clerk needs your phone number, write it on the check. Never give it out loud for strangers to hear.
- Do not allow sales clerks to write your credit card number on your check.
- Never write down personal identification numbers (PINS) or passwords. Memorize them!

- Order a copy of your credit report at least once a year from each of the three major credit bureaus. Review each report to verify that the information is correct and that there are no fraudulent transactions. You can also purchase services that alert you when there are irregularities in your accounts. Check with the three major credit report agencies for further information on these services.

- Only shop at Internet sites that have a secure server. Secure pages begin with "https" instead of "http." A picture of a lock in the locked position should appear on the browser window.



- When you subscribe to an online service, you may be asked to give credit card information. Be aware of con artists who may ask you to confirm your enrollment when entering an interactive services site. Don't give out your password, credit card or checking account numbers! Contact your service provider to report such activity.

Equifax www.equifax.com

- Fraud Alert (800) 525-6285
- Credit Report (800) 685-1111

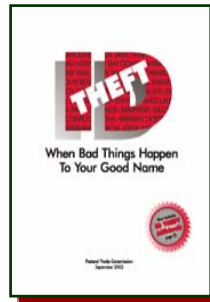
Experian www.experian.com

- Fraud Alert (888) 397-3742
- Credit Report (800) 360-7540

Trans Union www.transunion.com

- Fraud Alert (800) 680-7289
- Credit Report (800) 888-4213

Order a credit report for your child and/or a deceased family member; anyone can be a victim of Identity Theft!



For additional information on Identity Theft or to obtain a copy of "When Bad Things Happen To Your Good Name", visit the Federal Trade Commission's website at: www.ftc.gov

Internet Crime:

For additional information on filing a report pertaining to Identity Theft and other crime that occurred **online**, visit the FBI's Internet Crime Complaint Center website at: www.ic3.gov

For further information on crime prevention please call the Newport Beach Crime Prevention Unit at (949) 644-3699.

Visit us on the Web at www.nbpd.org

Minimizing your risk on-line:

- Limit the amount of information you give out over the Internet (i.e. genealogy sites)
- Use your credit card instead of your debit card when purchasing merchandise through the Internet.



Newport Beach Police Department

Tips To Minimize Your Risk of Identity Theft