- ✓ Shield your hand when punching in your PIN number.
- ✓ Memorize your social security number and all of your passwords. Do not record them on any cards or anything in your wallet or purse.
- ✓ Sign all new credit cards upon receipt.
- ✓ Save all credit card receipts and match them against your monthly bills.
- ✓ Notify your credit card companies and financial institutions in advance of any change of address or phone number.
- ✓ Never loan your credit cards to anyone.
- ✓ Never put your credit card or any other financial account number on a postcard or on the outside of an envelope.
- ✓ If you applied for a new credit card and it hasn't arrived in a timely manner, call the bank or credit card company involved.
- ✓ Report all lost or stolen credit cards immediately.
- ✓ Closely monitor expiration dates on your credit cards. Contact the credit card issuer if replacement cards are not received prior to the expiration dates.
- ✓ Beware of mail or telephone solicitations disguised as promotions offering instant prizes or awards designed solely to obtain your personal information or credit card numbers.

Internet and On-line Service

- ✓ Use caution when disclosing checking account numbers, credit card numbers or other personal financial data at any Web site or on-line service location unless you receive a secured authentication key from your provider.
- ✓ When you subscribe to an on-line service, you may be asked to give credit card information. When you enter any interactive service site, beware of con artists who may ask you to "confirm" your enrollment service by disclosing passwords or the credit card account number used to subscribe. Don't give them out.

Santa Rosa Police Dept. Case #_____

Make a note of this case number in your detailed history folder and reference it when you have contact with any business or law enforcement agency concerning this report. Depending upon the location (jurisdiction) of where the crime occurred (goods or services obtained or delivered), an investigator may or may not be assigned to this case.

If the crime occurred in Santa Rosa and there are workable leads, such as witnesses and suspect information, an investigator will be assigned to the case. Unfortunately, if there are no significant leads to identify the suspect, an officer will not be assigned to the case.

Notes:_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

INFORMATIONAL WEB SITES

Federal Trade Commission
www.ftc.gov

California Dept. of Consumer Affairs
www.dca.ca.gov

Privacy Rights Clearing House
www.privacyrights.org

U.S. Government Accounting Office
www.gao.gov

U.S. Postal Inspection Service
www.usps.gov/postalinspectors

International Association of
Financial Crimes Investigators
www.iafci.org
(go to links section)

www.equifax.com
www.experian.com
www.tuc.com

Santa Rosa
Police Department
965 Sonoma Avenue
Santa Rosa, CA 95404
www.santarosapd.com

CITY OF SANTA ROSA

IDENTITY THEFT

A Quick Reference Guide

PC 530.5: Unauthorized Use of Personal Identifying Information

(a) Every person who willfully obtains personal identifying information, as defined in subdivision (b), of another person without the authorization of that person, and uses that information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services, or medical information in the name of the other person without the consent of that person is guilty of a public offense.

Identity Theft

Identity theft involves acquiring key pieces of someone's identifying information, such as name, address, date of birth, social security number and mother's maiden name, in order to impersonate them. This information enables the identity thief to commit numerous forms of fraud which include, but are not limited to, taking over the victim's financial accounts, opening new bank accounts, purchasing automobiles, applying for loans, credit cards and social security benefits, renting apartments, and establishing services with utility and phone companies.

How does Identity Theft occur?

- Theft of wallet/purse containing your ID, credit or bank cards.
- Theft of mail (bank/credit card statements; pre-approved credit applications).
- Change of address forms can be completed by a thief using your information.
- Personal data can be retrieved from your trash cans.
- Credit reports or personal information can be obtained by a thief posing as a landlord or employer.
- If you've been burglarized, personal information can be used by a thief.
- Personal information can be bought from "inside sources" (internet).

What to do if you become a victim:

✓ Contact all creditors by phone and in writing to inform them of the problem.

Sample Creditor Letter

Dear (Creditor's Name):

On (date), I received your letter demanding payment of ($amount). I did not open this account and incur this unpaid balance. Someone other than myself wrongfully used my personal information to obtain a line of credit/service. Your company extended a line of credit/services to someone other than myself. Your company is a victim and should file a police report in the appropriate jurisdiction.

You are hereby notified that on (date), I filed an identify theft report with the Santa Rosa Police Department, case #. A copy of which can be obtained by contacting the Records Department at (707) 543-3600.

Sincerely,
Your name & address

✓ Set up a folder to keep a detailed history of this crime.

✓ Keep a log of all your contacts and make copies of all documents.

✓ Notify the US Postal Inspector if your mail has been stolen or tampered with:
- US Postal Inspection Service – Local Post Office - (see phone listing under Federal Government)
- www.usps.gov/websites/depart/inspect

✓ Contact the Federal Trade Commission to report the problem:
- www.ftc.gov - The FTC is the federal clearing house for complaints by victims of identity theft. The FTC helps victims by providing information to help resolve financial and other problems that could result from identity theft. Their hotline telephone number is 1-877-IDTHEFT (438-4338).

✓ Call each of the three credit bureaus' fraud units to report identity theft. Ask to have a "Fraud Alert/Victim Impact" statement placed in your credit file asking that creditors call you before opening any new accounts.

CREDIT BUREAUS

Equifax
P.O. Box 105069
Atlanta , GA 30348
Order Report: (800) 685-1111
Report Fraud: (800) 525-6285

Experian
P.O. Box 1017
Allen, TX 75013-0949
Order Report: (888) 397-3742
Report Fraud: (888) 397-3742

Trans Union
P.O. Box 6790
Fullerton, CA 92834
Order Report: (800) 916-8800
Report Fraud: (800) 680-7289

✓ Request that a copy of your credit report be sent to you.

✓ Alert your banks to flag your accounts and contact you to confirm any unusual activity. Request a change of PIN and a new password.

✓ If you have any checks stolen or bank accounts set up fraudulently, report it to the following companies:
- National Check Fraud Service – (843) 571-2143
- SCAN – (800) 262-7771
- TeleCheck – (800) 710-9898
- Chexsystesm – (800) 428-9623
- CheckRite – (800) 766-2748
- CrossCheck – (707) 586-0551
- Equifax Check Systems– (800) 437-5120
- International Check Services – (800) 526-5380

✓ Contact the Social Security Administration's Fraud Hotline–(800) 269-0271 Earnings/Benefits Statement – (800) 772-1213.

✓ Contact the state office of the Department of Motor Vehicles at (866) 658-5758 to see if another license was issued in your name. If so, request a new license number and fill out the DMV's complaint form to begin the fraud investigation process.

✓ Obtain description of suspect (if known).

✓ Obtain witness information.

✓ Determine the financial loss to you. Attach all supporting documentation.

Preventative Actions

✓ Promptly remove mail from your mailbox after delivery.

✓ Deposit outgoing mail in post office collection mailboxes or at your local post office. Do not leave in unsecured mail receptacles.

✓ Never give personal information over the telephone (social security number, date of birth, mother's maiden name, credit card number, or bank PIN code) unless you initiated the phone call. Protect this information and release it only when absolutely necessary.

✓ Shred pre-approved credit applications, credit card receipts, bills, and other financial information you don't want before discarding them in the trash or recycling bin.

✓ Order your credit report from the three credit bureaus quarterly to check for fraudulent activity or other discrepancies.

✓ Never leave receipts at bank machines, bank counters, trash receptacles, or unattended gasoline pumps. Keep track of all your paperwork. When you no longer need it, destroy it.