WHAT TO DO IF YOU'RE A VICTIM

- Contact all creditors by phone and in writing to inform them of the problem.
- Set up a folder to keep a detailed history of the 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.
- Contact the Federal Trade Commission to report the problem.
- Call 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.
- Request 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.
- Obtain a description of the suspect if known.
- Obtain witness information.
- Determine the financial loss to you. Attach all supporting documentation.
- Contact the Social Security Fraud Hotline at (800) 269-0271, and Earnings/Benefits Statement at (800) 772-1213.
- Contact 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.
- Contact the Identity Theft Council to help you fix Identity Theft problems. It's a free service endorsed by Bay Area law enforcement to help victims of Identity Theft: (888) 771-0767.
- If you have checks stolen or bank accounts set up fraudulently, report it to the following:
  - ✓ National Check Fraud: (843) 571-2143
  - ✓ SCAN: (800) 262-7771
  - ✓ TeleCheck: (800) 710-9898
  - ✓ Chexsystem: (800) 428-9623
  - ✓ CrossCheck: (707) 665-2100

INFORMATIONAL WEBSITES

- Identity Theft Council: www.identitytheftcouncil.org
- Federal Trade Commission: www.ftc.gov
- California Department of Consumer Affairs: www.dca.ca.gov
- Privacy Rights Clearinghouse: www.privacyrights.org
- U.S. Government Accountability: www.gao.gov
- U.S. Postal Inspection Service: www.postalinspectors.uspis.gov
- International Association of Financial Crimes Investigators: www.iafci.org

CREDIT BUREAUS

Equifax
P.O. Box 740241, Atlanta, GA 30374
Order Report: (800) 685-1111
Report Fraud: (800) 525-6285
www.equifax.com

Experian
Order Report or Report Fraud: (888) 397-3742
www.experian.com

TransUnion
P.O. Box 105281, Atlanta, GA 30348
Order Report: (877) 322-8228
Report Fraud: (800) 680-7289
http://www.transunion.com

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 me wrongfully used my personal information to obtain a line of credit/service. Your company extended a line of credit/service to someone other than me. 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 identity theft report with the Santa Rosa Police Department, case #_____, a copy of which can be obtained by contacting the Records Bureau at (707) 543-3600.
Sincerely, (Your name and address)

SANTA ROSA POLICE DEPARTMENT

IDENTITY THEFT

A Quick Reference Guide

Santa Rosa Police Department
965 Sonoma Avenue
Santa Rosa, CA 95404

Emergency: 9-1-1
Main Phone: 707-543-3600
Non-Emergency: 707-528-5222
Website: www.santarosapd.com

IDENTITY THEFT INFORMATION

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 I.D. THEFT OCCUR?

- Theft of a wallet or 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 can.
- 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).

PREVENTATIVE ACTIONS

- Never loan your credit cards to anyone.
- Report all lost or stolen credit cards immediately.
- Deposit outgoing mail in a post office collection mailbox or at your local post office. Do not leave in an unsecured mail receptacle.
- Promptly remove mail from your mailbox after delivery.
- 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 no longer needed, destroy it.
- Shield your hand when entering your PIN number.
- Memorize your social security number and all of your passwords. Don't 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 put credit card or other financial account numbers on a postcard or 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.
- Closely monitor expiration dates on your credit cards. Contact the credit card issuer if replacement cards are not received prior to the expiration date.
- 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 of other personal financial data on any website 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.

FILING A POLICE REPORT

Make a note of the police report 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 the 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 may not be assigned.