

RESOURCES

Credit Reporting Bureaus:

Equifax: PO Box 740256, Atlanta, GA 30374
Report Fraud: call (800) 525-6285 and write to the address above
Order a credit report (800) 685-1111
www.equifax.com

Experian PO Box 1017 Allen, TX 75013-1017
Report Fraud: call (888) 397-3742 and write to the address above
Order a credit report (888) 397-3742
www.experian.com

Trans Union: PO Box 6790 Fullerton, CA 92834
Report Fraud: call (800) 680-7289 Consumer Relations: (800) 916-8800 and write to Fraud Victim Assistance Division, PO Box 6790, Fullerton, CA 92834-6790
Order a credit report (800) 888-4213
www.transunion.com

Opt out of pre-approved offers of credit

(888) 5OPTOUT or (888) 567-8688. Remember, if you have been the victim of credit fraud, identity theft, or are denied credit, you are entitled to a free credit report. If you are a victim of fraud, be sure to ask the credit bureaus for free copies. Examine each of the credit reports as some fraudulent activity may have been reported to one of the credit bureaus and not the other(s). Different credit bureaus occasionally receive reports from different sources and not all creditors report to all of the credit bureaus.

Social Security Administration

Report Fraud (800) 269-0271
Order your Earnings and Benefits Statement: (800) 772-1213
www.ssa.gov

To remove your name from mail and phone lists:

Direct Marketing Association
Mail Preference Service, PO Box 9008,
Farmingdale, NY 11735
Telephone Preference Service, PO Box 9014,
Farmingdale, NY 11735

To report fraudulent use of your checks:

CheckRite:	(800) 766-2748
CrossCheck:	(707) 586-0551
Chexsystems:	(800) 428-9623
Equifax:	(800) 525-6285
International Check Svcs:	(800) 526-5380
SCAN:	(888) 262-7771
Telecheck:	(800) 710-9898
National Ck Fraud Ctr:	(843) 571-2143

Other Useful Resources:

Federal Government Information Center:
Call (800) 688-9889 for help in obtaining government agency phone numbers

Federal Trade Commission (877) FTC-HELP, or (877) ID-THEFT
FTC web address: www.ftc.gov, or
www.consumer.gov/idtheft

CALPIRG (The Consumer Advocate)
(213) 251-3680
www.calpirg.org

Privacy Rights Clearinghouse (619) 298-3396
www.privacyrights.org

CA Dept of Justice <http://ag.ca.gov/idtheft/>
CA Dept of Consumer Affairs:
www.privacy.ca.gov

United States Postal Service
US Postal Inspector (626) 405-1200
www.usps.gov/postalinspectors

Free annual credit report:
www.annualcreditreport.com

Laws

Federal

Identity Theft and Assumption Deterrence Act
Public Law 105-318, 112 Stat. 3007 (Oct. 30, 1998)
Fair Credit Reporting Act (FCRA)
15 U.S.C. Section 1681 et seq.

State of California

Unauthorized Use of Personal Identifying Information - Penal Code Section 530.5

IF YOU ARE THE VICTIM OF

IDENTITY THEFT

WHAT TO DO IF IT HAPPENS TO YOU



RIVERSIDE SHERIFF'S DEPARTMENT

STANLEY SNIFF, SHERIFF-CORONER

(951) 955-2400 • www.riversidesheriff.org

This guide provides victims of identity theft with the major resources to contact. Victims themselves have the ability to assist greatly with resolving their case. It is important to act quickly and assertively to minimize the damage.

In dealing with the authorities and with financial institutions and creditors, keep a log of all conversations including the dates, times, names of subjects with whom you speak and phone numbers for contact. Note the time spent and any expenses incurred. Confirm conversations in writing. Send correspondence by certified mail (return receipt requested). Keep copies of all letters and documents both received by you and sent by you.

Once you discover or suspect you are a victim of identity theft you should do the following:

- 1. Credit Bureaus** - Immediately call any one of the three credit reporting bureaus—Equifax, Experian, or Trans Union—and report the theft of your compromised credit accounts and personal identifying information. As a service to you, their fraud representative will contact the other credit reporting bureau's on your behalf. The phone numbers for each of the credit bureaus is provided at the end of this brochure. You can request that your account be flagged with a "fraud alert" or you may request a "credit freeze." These services are free to victims of identity theft. You may also add a victim's statement to your credit report (up to 100 words) such as, "*My ID has been used to apply for credit fraudulently. Contact me at (your phone number) to verify all applications prior to granting credit.*) Be sure to ask how a

fraud alert or credit freeze will impact your account. Be aware that these measures may not entirely stop new fraudulent accounts from being established using your identity by an imposter. Ask the credit bureaus for names and phone numbers of credit grantors with whom fraudulent accounts have been opened. Ask the credit bureaus to remove the inquiries that have been generated due to the fraudulent access. You may also ask the credit bureaus to notify those who have received your credit report in the last six months in order to alert them to the disputed and erroneous information (two years for employers). In an effort to prevent credit fraud and identity theft, you are entitled to receive a free copy of your credit report once a year so you can monitor your reports for fraudulent activity.

2. Creditors - Contact all creditors immediately with whom your name has been used fraudulently—by phone and in writing. Get replacement cards with new account numbers for your accounts that have been used fraudulently. Ask that old accounts be processed as "account closed at consumer's request." This is better than "card lost or stolen" because when this statement is reported to credit bureaus it can be interpreted as blaming you for the loss. Carefully monitor your mail and credit card bills for evidence of new fraudulent activity. Report it immediately to credit grantors.

3. Law Enforcement - Report the crime to the law enforcement agency that has jurisdiction where you live. Should the investigation reveal the suspect lives outside your jurisdiction, the matter will be forwarded to the appropriate agency for follow-up investigation. Give them as much documented evidence as possible. Get a copy of your police report. Keep the report number of your police report handy and give it to creditors and others who require verification of your case. Credit card companies and banks may require you to show the report to verify the crime. Some police departments have been known to resist writing reports on such crimes. Prior to January 1st, 1998, the creditors (credit card companies, banks, etc) were the only "legal" victims of Credit Fraud/Identity Theft. California Penal Code Section 530.5 went into effect on January 1st, 1998, thus giving legal standing to individual victims. Some police departments have not yet received training in the new laws of identity theft. Be persistent.

4. Stolen Checks - If you have had checks stolen or bank accounts set up fraudulently, report it to the check verification companies. Put stop payments on any outstanding checks that you are unsure of. Cancel your checking and savings accounts and obtain new account numbers. Give the bank a secret password for your account (not your mother's maiden name).

5. ATM/Debit Cards - If your ATM card has been stolen or is compromised, get a new card, account number, and password. Do not use your old password. When creating a password don't use common numbers like the last four digits of your social security number or your date of birth.

6. Fraudulent change of address - Notify the local Postal Inspector if you suspect an identity thief has filed a change of address with the post office or has used the mail to commit credit or bank fraud. Find out where the fraudulent credit cards were sent. Notify the local Postmaster for the address to forward all mail in your name to your own address. You may also need to talk to the mail carrier.

7. Social Security Number Misuse - Call the Social Security Administration to report fraudulent use of your social security number. As a last resort, you might want to change the number. The SSA will only change it if you fit their fraud victim criteria. Also, order a copy of your Earnings and Benefits Statement and check it for accuracy.

8. Passports - If you have a passport, notify the passport office in writing to be on the lookout for anyone ordering a new passport fraudulently.

9. Phone Service - If your long distance calling card has been stolen or you discover fraudulent charges on your bill, cancel the account and open a new one. Provide a password which must be used anytime the account is changed.

10. Driver License Number Misuse - You may need to change your driver's license number if someone is using your number as identification on bad checks. Call the state office of the Department of Motor Vehicles (DMV) to see if any other licenses have been issued in your name. Put a fraud alert on your license. Go to your local DMV to request a new number. Also, fill out the DMV's complaint form to begin the fraud investigation process. Send supporting documents with the complaint form to the nearest DMV investigation office.

11. False Civil and Criminal Judgments - Sometimes victims of identity theft are wrongfully accused of crimes committed by the imposter. If a civil judgment has been entered in your name for actions taken by your imposter, contact the court where the judgment was entered and report that you were a victim of identity theft. If you were wrongfully prosecuted for criminal charges, contact the state Department of Justice and the FBI. Ask how to clear your name.

Creditors may request for you to fill out and notarize fraud affidavits which could become costly. The law does not require that a notarized affidavit be provided to creditors. A

written statement and a copy of the police report should be sufficient.

If you believe your mail has been stolen, you may report this to your local Postmaster or the nearest Postal Inspector. You will be asked to complete a PS Form 2016, Mail Theft and Vandalism Complaint. Analysis of these forms helps Postal Inspectors determine if the theft of your mail is isolated or part of a larger mail theft problem in your neighborhood.

Although inconvenient, you may want to consider taking your outgoing mail to the local post office rather than leaving it in your residential mail box. Never leave your delivered mail in your mail box for excessive periods of time, including overnight. Many mail thieves operate at night and take mail left unattended in boxes.

You may want to consult an attorney to determine if you should take legal action against creditors and/or credit bureaus if they do not cooperate in removing fraudulent entries from your credit report or if negligence is a factor. Call the local Bar Association to find an attorney who specializes in Consumer Law and the Fair Credit Reporting Act.

A victim's information can be stolen and misused, in much the same way a burglary victim's property is stolen from his/her home. This is an information crime—personal identifying information is often taken and the victim's financial reputation is often harmed. The jurisdiction for reporting the crime of Identity Theft is where the impersonated victim resides. **Penal Code Section 530.5** provides that *every person who willfully obtains personal identifying information for any unlawful purpose including obtaining or attempting 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.*

Personal identifying information, as used in this section, means the *name, address, telephone number, driver's license number, social security number, place of employment, employee identification number, mother's maiden name, demand deposit account number, savings account number or credit card number* of an individual person.

If there are workable leads such as possible witness or suspect information, an investigator may be assigned to the case. If the investigator determines the suspected crime(s) was committed in a different jurisdiction, the matter may be referred to the appropriate law enforcement agency with jurisdiction for investigation of the facts. YOU are the only one who can clear your credit report. Due to privacy laws, creditors cannot share information regarding your accounts—even fraudulent ones—until you have personally notified the creditor of the fraudulent nature of the account(s).