

## **IDENTITY THEFT: What to do if it happens to you**

Copyright © 1997-2003. Utility Consumers' Action Network / Privacy Rights Clearinghouse and CALPIRG Charitable Trust. Released Jan. 1997. Revised April 2003.  
A Joint Publication of the Privacy Rights Clearinghouse and CALPIRG

**This guide provides victims of identity theft with the major resources to contact. Unfortunately, at this time victims themselves are burdened with resolving the problem. You must act quickly and assertively to minimize the damage.**

**In dealing with the authorities and financial institutions, keep a log of all conversations, including dates, names, and phone numbers. Note time spent and expenses incurred in case you are able to seek restitution in a later judgment or conviction against the thief, if you itemize tax deductions for theft-related expenses (consult your accountant). Confirm conversations in writing. Send correspondence by certified mail, return receipt requested. Keep copies of all letters and documents.**

**1. Credit bureaus.** Immediately report the situation to the fraud units of the of the three credit reporting companies—Experian (formerly TRW), Equifax and TransUnion. As of April 2003, if you notify one bureau that you are a victim of identity theft, it will notify the other two. Report that your identifying information is being used by another person to obtain credit fraudulently in your name. Ask that your file be flagged with a fraud alert. Add a victim's statement to your report. ("My ID has been used to apply for credit fraudulently. Contact me at [your phone number] to verify all applications.")

Each credit bureau will mail you a free credit report once you have called them to flag your file with a fraud alert. Fraud alerts are usually placed for 90-180 days. You will want to extend the time period to seven years. Do so in writing following the directions sent in the credit report you receive. You may cancel fraud alerts at any time. In all communications with the credit bureaus, you will want to refer to the unique number assigned to your credit report and use certified, return receipt mail. Be sure to save all credit reports as part of your fraud documentation.

Ask the credit bureaus for names and phone numbers of credit grantors with whom fraudulent accounts have been opened if this information is not included on the credit report. Ask the credit bureaus in writing to remove 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). Under California law, when you provide your police report to the credit bureaus, they must remove the fraudulent accounts from your credit report (Calif. Civil Code 1785.16(k). (see #3 below.)

Be aware that these measures will not entirely stop new fraudulent accounts from being opened by the imposter. Credit issuers are not required by law to observe fraud alerts. Request a free copy of your credit report every few months so you can monitor for fraud. Under a new California law, victims are able to receive one free report each month for the first 12 months upon request. (California Civil Code 1785.15.3, effective July 1, 2003.) In other states, you may be charged after the first report. Still it is important to check your credit report about every three months during the active phase of the crime.

California law now enables individuals to place a "security freeze" on their credit reports. This essentially prevents anyone from accessing your credit file for any reason, until and unless you instruct the credit bureaus to unfreeze or "thaw" your report. It provides more protection than a fraud alert. If your identity thief is particularly aggressive and gives no indication of ceasing to use your identity to obtain credit, and if you live in California, you should consider using the security freeze to curtail access to your credit file. The security freeze is free to victims of identity theft. Non-victims who wish to use the security freeze for prevention purposes must pay a fee to activate the freeze.

The web site of the California Office of Privacy Protection provides information on how to establish a security freeze, [www.privacy.ca.gov/financial/cfreeze.htm](http://www.privacy.ca.gov/financial/cfreeze.htm).

**2. Creditors.**—New Accounts—Contact all creditors immediately with whom your name has been used fraudulently, by phone and in writing. You will see evidence of these accounts on your credit reports. Creditors will likely ask you to fill out fraud affidavits. The Federal Trade Commission provides a uniform affidavit form that most creditors accept.

(Web: [www.consumer.gov/idtheft/affidavit.htm](http://www.consumer.gov/idtheft/affidavit.htm)). No law requires affidavits to be notarized at your own expense. You may choose to substitute witness signatures for notarization if creditors require verification of your signature.

Ask the credit grantors to furnish you and your investigating law enforcement agency copies of the documentation, such as the application and transaction records, showing the fraudulent transactions. In California, they are required by law to give you these copies (California Penal Code 530.8). The California Office of Privacy Protection provides instructions and sample letters on how to obtain documentation from credit grantors, [www.privacy.ca.gov/fair.htm](http://www.privacy.ca.gov/fair.htm).

**2a. Creditors.**—Existing Accounts—If your existing credit accounts have been used fraudulently, get replacement cards with new account numbers. Ask that old accounts be processed as "account closed at consumer's request" (better than "card lost or stolen" because it can be interpreted as blaming you.) Monitor your mail and bills for evidence of new fraudulent activity. Report it immediately to creditor grantors. Add passwords to all accounts. This should not be your mother's maiden name or a word that is easily guessed.

**3. Debt collectors.** If debt collectors attempt to require you to pay the unpaid bills on fraudulent credit accounts, ask for the name of the company, the name of the person contacting you, phone number, and address. Tell the collector that you are a victim of fraud and are not responsible for the account. Ask the collector for the name and contact information for the referring credit issuer, the amount of the debt, account number, and dates of the charges. Ask if they need you to complete their fraud affidavit form or if you can use the Federal Trade Commission form (see #2 above). Follow up in writing to the debt collector explaining your situation. Ask that they confirm in writing that you do not owe the debt and that the account has been closed. (For additional information on dealing with debt collectors, read Fact Sheet No. 116 of the Identity Theft Resource Center, [www.idtheftcenter.org](http://www.idtheftcenter.org) under "Victim Resources.")

**4. Law enforcement.** Report the crime to your local police or sheriff's department. You might also need to report it to police departments where the crime occurred. Give them as much documented evidence as possible. Make sure the police report lists the fraud accounts. Get a copy of the report. Keep the phone number of your investigator 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 in order to verify the crime. It is a violation of federal law (18 USC 1028) and the laws of many states (such as Calif. Penal Code 530.5) to assume someone's identity for fraudulent purposes. (Web site for state laws: [www.consumer.gov/idtheft/statelaw.htm](http://www.consumer.gov/idtheft/statelaw.htm)). Some police departments don't write reports on such crimes, so be persistent! Also report to the Federal Trade Commission (see end of guide).

**5. Stolen checks.** If you have had checks stolen or bank accounts set up fraudulently, report it to the appropriate check verification companies (see end). Your bank branch should be able to provide you with a fraud affidavit. 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 mother's maiden name). If your own checks are rejected at stores where you shop, contact the check verification company that the merchant uses (see end of guide).

**6. ATM cards.** If your ATM or debit card has been stolen or compromised, report it immediately. Contact your bank branch and request a fraud affidavit. 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 (SSN) or your birth date. Monitor your account statement. You may be liable if fraud is not reported quickly. Be sure to read the debit card contract for liability. Some cards are better protected in cases of fraud than others.

**7. Fraudulent change of address.** Notify the local Postal Inspector if you suspect an identity thief has filed a change of your address with the post office or has used the mail to commit fraud. (Call the U.S. Post Office to obtain the phone number, (800) 275-8777.) Find out where fraudulent credit cards were sent. Notify the local Postmaster for that address to forward all mail in your name to your own address. You may also need to talk with the mail carrier. (Web: [www.usps.gov/websites/depart/inspect](http://www.usps.gov/websites/depart/inspect))

**8. Secret Service jurisdiction.** The Secret Service has jurisdiction over financial fraud. But, based on U.S. Attorney guidelines, it usually does not investigate individual cases unless the dollar amount is high or you are one of many victims of a fraud ring. To interest the Secret Service in your case, you may want to ask the fraud department of the credit card companies and/or banks, as well as the police investigator, to notify the Secret Service agent they work with. (Web: [www.treas.gov/usss](http://www.treas.gov/usss))

**9. Social Security Number (SSN) misuse.** Contact the Social Security Administration (SSA) to report fraudulent use of your SSN such as welfare or Social Security benefit fraud. They do not handle cases of financial or criminal identity theft. (See contact information at the end of this guide.) As a last resort, you might try to change your number, although we don't recommend it except for very serious cases. The SSA will only change the number if you fit their fraud victim criteria. See Fact Sheet 113 ("Victim Resources") at [www.idtheftcenter.org](http://www.idtheftcenter.org) for more information on this topic. (Web: [www.ssa.gov](http://www.ssa.gov))

**10. Passports.** Whether you have a passport or not, write the passport office to alert them to anyone ordering a passport fraudulently (see address at end). (Web: [www.travel.state.gov/passport\\_services.html](http://www.travel.state.gov/passport_services.html))

**11. Phone service.** Provide a password which must be used any time your local, cell, and long distance accounts are changed. In California, SBC/Pacific Bell's fraud hotline is (877) 202-4558. If your calling card has been stolen or there are fraudulent charges, cancel it and open a new account.

**12. Driver's license number misuse.** You may need to change your driver's license number if someone is using yours as ID on bad checks or for other types of fraud. Call the state office of the Department of Motor Vehicles (DMV) to see if another license was issued in your name. Put a fraud alert on your license if your state's DMV provides a fraud alert process. Go to your local DMV to request a new number. Fill out the DMV's complaint form to begin the investigation process. Send supporting documents with the completed form to the nearest DMV investigation office. Web: [www.aamva.org/links/mnu\\_linkJurisdictions.asp](http://www.aamva.org/links/mnu_linkJurisdictions.asp).

**13. Victim statements.** If the imposter is apprehended by law enforcement and stands trial, write a victim impact letter to the judge handling the case. Contact the victim-witness assistance program in your area for further information on how to make your voice heard in the legal proceedings. (Read Fact Sheet 111 on victim impact statements at [www.idtheftcenter.org](http://www.idtheftcenter.org) under "Victim Resources.")

**14. False civil and criminal judgments.** Sometimes victims of identity theft are wrongfully accused of crimes committed by the imposter. If a civil judgment is entered in your name for your imposter's actions, contact the court where the judgment was entered and report that you are a victim of identity theft. If you are wrongfully arrested or prosecuted for criminal charges, contact the police department and the court in the jurisdiction of the arrest. Also contact the state Department of Justice and the FBI. Ask how to clear your name. See PRC Fact Sheet 17g, [www.privacyrights.org/fs/fs17g-CrimIdTheft.htm](http://www.privacyrights.org/fs/fs17g-CrimIdTheft.htm).

**15. Legal help.** You may want to consult an attorney to determine legal action to take against creditors and/or credit bureaus if they are not cooperative in removing fraudulent entries from your credit report or if negligence

is a factor. Call the local Bar Association, or Legal Aid office in your area (for low-income households), or the National Association of Consumer Advocates ([www.naca.net/resources.htm](http://www.naca.net/resources.htm)) to find an attorney who specializes in consumer law, the Fair Credit Reporting Act and the Fair Credit Billing Act. If you are a senior citizen or take care of a dependent adult, be sure to look under Elder Law or Aging and Independent Services for referral centers.

**16. Other forms of identity theft.** If a deceased relative's information is being used to perpetrate identity theft, or if you personally know the thief, additional information about how to address these situations is available in other fact sheets. See [www.idtheftcenter.org/vguides.shtml](http://www.idtheftcenter.org/vguides.shtml)

**17. Dealing with emotional stress.** Psychological counseling may help you deal with the stress and anxiety commonly experienced by victims. Know that you are not alone. Contact the Identity Theft Resource Center for information on how to network with other victims and deal with the impact of this crime. Web: [www.idtheftcenter.org](http://www.idtheftcenter.org) (Fact Sheet 108, "Victim Resources")

**18. Making change.** Write to your state and federal legislators. Demand stronger privacy protection and prevention efforts by creditors and credit bureaus.

**19. Don't give in.** Do not pay any bill or portion of a bill that is a result of fraud. Do not cover any checks that were written or cashed fraudulently. Do not file for bankruptcy. Your credit rating should not be permanently affected. No legal action should be taken against you. If any merchant, financial company or collection agency suggests otherwise, restate your willingness to cooperate, but don't allow yourself to be coerced into paying fraudulent bills. Report such attempts to government regulators immediately.

### **Credit Reporting Bureaus**

#### **Equifax:**

P.O. Box 105069, Atlanta, GA 30348

[www.equifax.com](http://www.equifax.com)

Report fraud: Call (800) 525-6285 and write to the address above. Order

credit report: (800) 685-1111

TDD: (800) 255-0056

Web: [www.equifax.com](http://www.equifax.com)

#### **Experian (formerly TRW):**

P.O. Box 9532, Allen, Texas 75013

Report fraud: Call (888) EXPERIAN (888-397-3742) and write to address

above. Order credit report: (888) EXPERIAN

To report fraud: 888-397-3742

TDD: Use relay to fraud number above

Web: [www.experian.com](http://www.experian.com)

#### **TransUnion:**

P.O. Box 6790, Fullerton, CA 92834.

Report fraud: (800)-680-7289 and write to address above. Order credit

report: (800) 888-4213

TDD:(877)-553-7803

E-mail (fraud victims only): [fvd@transunion.com](mailto:fvd@transunion.com)

Web: [www.transunion.com](http://www.transunion.com)

- To opt out of pre-approved offers of credit for all three bureaus, call (888) 5OPTOUT (888-567-8688). You may choose a two-year opt-out period or permanent opt-out status.

- Remember, you are entitled to a free credit report if you are a victim of identity theft, if you have been denied credit, if you receive welfare benefits, or if you are unemployed.

### **Social Security Administration**

- Order Earnings & Benefits Statement: (800) 772-1213. The SSA automatically mails it to individuals three months before the birthday. Web: [www.ssa.gov/online/ssa-7004.html](http://www.ssa.gov/online/ssa-7004.html)
- Report fraud: (800) 269-0271. Web: [www.ssa.gov/oig/public\\_fraud\\_reporting/index.htm](http://www.ssa.gov/oig/public_fraud_reporting/index.htm) or write to: Social Security Administration, Office of the Inspector General, P.O. Box 17768, Baltimore, MD 21355.

### **U.S. State Department, Passport Office**

- U.S. Dept. of State, Passport Services, Consular Lost/Stolen Passport Section, 1111 19th St., NW, Suite 500, Washington, DC 20036

### **To remove your name from mail and phone marketing lists**

- Direct Marketing Association, Mail Preference Service, P.O. Box 643, Carmel, NY 10512. Web: [www.dmaconsumers.org](http://www.dmaconsumers.org). Online opt-out program costs \$5.00. It is free by mail.
- FTC's telemarketing Do Not call registry (888) 382-1222 Online registration: [www.donotcall.gov](http://www.donotcall.gov) See PRC Fact Sheets No. 4 and No. 5 on reducing junk mail and telemarketing calls Web: [www.privacyrights.org/fs/fs4-junk.htm](http://www.privacyrights.org/fs/fs4-junk.htm) and [www.privacyrights.org/fs/fs5-tmkt.htm](http://www.privacyrights.org/fs/fs5-tmkt.htm)

### **To report fraudulent use of your checks**

- CheckRite: (800) 766-2748
- Chexsystems:(800) 428-9623
- CheckCenter/CrossCheck: (800) 843-0760
- Certigy/Equifax: (800) 437-5120
- International Check Services: (800) 526-5380
- SCAN: (800) 262-7771
- TeleCheck: (800) 710-9898

### **Other useful resources**

- Federal Trade Commission (FTC). The FTC offers information for victims. File your case with the FTC Consumer Response Center. Include your police report number. Use the FTC uniform affidavit form. (877) IDTHEFT Web: [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)
- Privacy Rights Clearinghouse (PRC), 3100 - 5th Ave., Suite B, San Diego, CA 92103. Phone: (619) 298-3396. E-mail: [prc@privacyrights.org](mailto:prc@privacyrights.org). Web: [www.privacyrights.org](http://www.privacyrights.org).
- Identity Theft Resource Center, P.O. Box 26833, San Diego, CA 92196. Lists regional victim support groups on its web site. Offers many guides for victims. (858) 693-7935 Web: [www.idtheftcenter.org](http://www.idtheftcenter.org). E-mail: [itrc@idtheftcenter.org](mailto:itrc@idtheftcenter.org)
- FBI Internet Fraud Complaint Center, Web: [www.ifccfbi.gov](http://www.ifccfbi.gov)
- U.S. Dept. Of Justice, identity theft information. Web: [www.usdoj.gov/criminal/fraud/idtheft.html](http://www.usdoj.gov/criminal/fraud/idtheft.html)
- Identity Theft Survival Kit. Phone: (800) 725-0807. Web: [www.identitytheft.org](http://www.identitytheft.org)

This guide is a project of the Privacy Rights Clearinghouse and CALPIRG, nonprofit consumer advocacy organizations. We thank Linda Foley of the Identity Theft Resource Center and Mari Frank, Esq. for their assistance.