

# IDENTITY THEFT

## WHAT TO DO IF IT HAPPENS TO YOU:

### PART I

If you think you're a victim of fraud, contact your credit card issuers to close or "flag" your account(s), and call your bank to put an alert on your checking accounts.

Empty your wallets of extra credit card (and ID's) - or better yet, cancel the ones you don't really use and keep a list of the ones you do use.

Never give out personal information over the phone, such as your date of birth, mother's maiden name, credit card number(s), Social Security number or bank PIN code, except to someone you know or an established firm.

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

Financial institutions or businesses that handle personal information should protect consumers' privacy by storing such material securely and ensuring it has limited access. It is essential to shred such material before disposing of it.

Consider removing your name from the marketing list of the three major credit-reporting bureaus:

- Experian (formerly TRW) at 800-353-0809
- Equifax at 800-219-1251
- Trans Union at 800-241-2858

This reduces the number of pre-approved applications you receive in the mail.

Order your credit report once a year to check for accuracy or fraudulent use.

### WHO TO CALL FOR HELP

Report credit card fraud to the three major credit-reporting bureaus:

- Experian (formerly TRW) at 800-301-7195
- Equifax at 800-525-6285
- Trans Union at 800-680-7289

If you've had stolen or bank accounts set up fraudulently in your name, call these check guarantee companies:

- Telecheck at 800-366-2425
- National Processing Company at 800-525-5380.

They can flag your file so that counterfeit checks will be refused.

If your Social Security number was used fraudulently, report the problem(s) to the Social Security Administration's Fraud Hotline at 800-269-0271. In extreme cases of fraud, it may be possible for you to get a new Social Security number.

If fraudulent charges appear on your account, call the Consumer Credit Counseling Service at 800-388-2227 for help in clearing false claims from your credit report.

If you're a victim of identity theft that involves the U.S. Mail, call your nearest Postal Inspection Service office and your local police.

## WHAT TO DO IF IT HAPPENS TO YOU: PART II

(Reprinted with permission of NACM® Loss Prevention Dept)

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. It is important to 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. Confirm conversation in writing. Send correspondence by certified mail (return receipt requested). Keep copies of all letters and documents.

1. CREDIT BUREAUS. Immediately call the fraud units of the three credit reporting companies - Experian (formerly TRW), Equifax and Trans Union. Report the theft of your credit card or numbers. Ask that your account be flagged. Also, add a victim's statement to your report (i.e. "My ID has been used to apply for credit fraudulently. Contact me at my phone number to verify all applications.") Be sure to ask how long the fraud alert is posted on your account and how you can extend it if necessary.

Beware that these measures may not entirely stop new fraudulent accounts from being opened by the imposter. Ask the credit bureaus in writing to provide you with free copies every few months so you can monitor your credit report.

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 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).

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 own accounts that have been used fraudulently. Request 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.

Fraud Verifications Requirements. You may be asked by banks and credit grantors to fill out and notarize fraud affidavits, which could become costly. The law does not require you to provide a notarized affidavit. A written statement and supporting documentation should be enough (unless the creditor offers to pay for the notary). Overly burdensome requirements by creditors should be reported to the federal government authorities. For help in determining which agency to contact, call CALPIRG or the Privacy Rights Clearinghouse.

3. LAW ENFORCEMENT. Report the crime to your local Police and Sheriff's Departments with jurisdiction in your case. Give them as much documented evidence as possible. Get a copy of your police report. Keep the phone number or your fraud investigator handy and give it to creditors and others who require verifications of your case. Credit card companies and banks may require you to show the report in order to verify the crime. Some police departments have been known to refuse to write reports on such crimes. 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 mother's maiden name).

5. ATM CARDS. If your ATM or debit card has been stolen or compromised, report it immediately. 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 birth date.
6. 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 credit or bank fraud. (Call the local Postmaster to obtain the phone numbers.) 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.
7. SECRET SERVICE JURISDICTION. The Secret Service has jurisdiction over financial fraud, but 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 particular Secret Service agent they work with.
8. SOCIAL SECURITY MISUSE. Call the Social Security Administration to report fraudulent use of your Social Security number. As a last resort, you might want to try to change your number. The SSA will only change it, however, if you fit the fraud victim criteria. Also order a copy of your Earnings and Benefits Statement and check it for accuracy.
9. PASSPORTS. If you have a passport, notify the passport office in writing to be on the lookout for anyone ordering a new passport fraudulently.
10. 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 that must be used any time the account is changed.
11. DRIVER LICENSE NUMBER MISUSE. You may need to change your driver's license number if someone is using yours as identification on bad checks. 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. 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 completed form to the nearest DMV investigations office.

12. 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 are a victim of identity theft. If you are wrongfully prosecuted for criminal charges, contact the state Department of Justice and the FBI. Ask how to clear your name.
13. LEGAL HELP. You may want to consult an attorney to determine legal action to take against creditor 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 to find an attorney who specializes in consumer law and the Fair Credit Reporting Act.
14. 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 CALPIRG or the Privacy Rights Clearinghouse for Information on how to network with other victims.
15. MAKING CHANGE. Write to your state and federal legislators. Demand stronger privacy protections and fraud assistance by creditors and credit bureaus. Contact CALPIRG for information on any pending state Or federal legislation.
16. DON'T GIVE IN. Finally, do NOT pay any bill or portion of a bill, which is a result of identity theft. Do NOT cover any checks, which were written and/or cashed fraudulently. Do NOT file for bankruptcy. Your credit rating should not be permanently affected and no legal actions should be taken against you. If any merchant, financial institution or collections agency suggest otherwise, simply restate your willingness to cooperate, but don't allow yourself to be coerced into paying fraudulent bills.

## RESOURCES

### *Credit Reporting Bureaus*

➤ Equifax

P.O. Box 740241  
Atlanta, GA 30374-0241  
Report Fraud: (800) 525-6285  
Order Credit Report: (800) 685-1111  
Opt out of pre-approved offers of credit:(888) 567-8688  
Web site: [www.equifax.com](http://www.equifax.com)

➤ Experian (formerly TRW)

P.O. Box 9595  
Allen, TX 75013-9595  
Report Fraud: (800) 301-7195  
Order Credit Report: (888) 397-3742  
Opt out of pre-approved offers of credit and marketing  
list: (800) 353-0809  
Web site: [www.experian.com](http://www.experian.com)

➤ Trans Union

P.O. box 390  
Springfield, PA 19064  
Report Fraud: (800) 680-7289  
Write to: Fraud Victim Assistance Division, P.O. Box  
6790, Fullerton, CA 92634  
Other Credit Report: (800) 888-4213  
Opt out of pre-approved offers of credit and marketing  
lists: (888) 567-8688  
Web site: [www.tuc.com](http://www.tuc.com)

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 received welfare benefits, or if you are unemployed.

*Social Security Administration*

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

*To remove your name from mail lists:*

Direct Marketing Association  
Mail Preference Service  
P.O. Box 9008  
Farmingdale, NY 11735

*To remove your name from phone lists:*

Telephone Preference Service  
P.O. Box 9014  
Farmingdale, NY 11735

*To report fraudulent use of your checks:*

Check Rite: (800) 766-2748  
Chexsystems: (800) 428-9623  
CrossCheck: (707) 586-0431  
Equifax: (800) 437-5120  
Natl Processing Co: (800) 526-5380  
SCAN: (800) 262-7771  
TeleCheck: (800) 853-3243

*Other useful resources:*

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

11965 Venice Blvd  
Suite 408  
Los Angeles, CA 90066  
Web site: <http://www.pirg.org/calpirg>.

Find out about its support group, Victims of Identity Theft.  
Participate in the online victims discussion group, [voit-moderator@pirg.org](mailto:voit-moderator@pirg.org). cosponsored by the Privacy Rights Clearinghouse.

**PRIVACY RIGHTS CLEARINGHOUSE**

1717 Kettner Ave  
Suite 105  
San Diego, CA 92101  
Phone: (619) 298-3396  
Web site: <http://www.privacyrights.org>.  
Obtain its book, "The Privacy Rights Handbook" (Avon, 1997)