Identity Theft: What to Do if It Happens to You

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 any expenses incurred. Confirm conversations 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 cards or numbers. Ask that your account be flagged. Also, add a victim's statement to your report, up to 100 words. ("My ID has been used to apply for credit fraudulently. Contact me at 311-123-4567 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.

Be aware 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. 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.

Creditors requirements to verify fraud. 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 that a notarized affidavit be provided to creditors. 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 federal government authorities. For help in determining which agency to contact, call CALPIRG or the Privacy Rights Clearinghouse (see below).

3. Law enforcement. Report the crime to all 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 of your fraud 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. 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 (see next page for names and phone numbers). 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 card has been stolen or 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 birthdate.

6. Fraudulent change of address. Notify the local Postal Inspector if you suspect an identity thief has filed 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 number.) 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 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 your 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.

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 which must be used any time the account is changed.

11. Drivers 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 investigation 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 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 to find an attorney who specializes in consumer law and the Fair Credit Reporting Act. [You may call the Legal Assistance Office at 242-5084.]

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 protection 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. Your credit rating should not be permanently affected, and no legal action should be taken against you. If any merchant, financial institution or collection agency suggests 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: Call (800) 525-6285 and write to address above. Order credit report: (800) 685-1111. Opt out of pre-approved offers of credit: (800) 556-4711.

Experian (formerly TRW): P.O. Box 1017, Allen, TX 75013
Report fraud: Call (800) 301-7195 and write to address above. Order credit report: (800) 682-7654. Opt out of pre-approved offers of credit and marketing lists: (800) 353-0809.

Trans Union: P.O. Box 390, Springfield, PA 19064
Report fraud: (800) 680-7289 and write to Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634. Order credit report: (800) 916-8800. Opt out of pre-approved offers of credit and marketing lists: (800) 680-7293.

Remember, if you have been 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. They will often provide them. Starting October 1997, free annual credit reports for victims of identity theft will be required by federal law.

*** Social Security Administration
Report fraud: (800) 269-0271. Order your Earnings and Benefits Statement: (800) 772-1213.

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

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

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

*** To report fraudulent use of your checks
CheckRite: (800) 766-2748
Chexsystems: (800) 428-9623
Equifax: (800) 437-5120
National Processing Co.: (800) 526-5380
SCAN: (800) 262-7771
TeleCheck: (800) 710-9898

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

CALPIRG, 11965 Venice Blvd., Suite 408, Los Angeles, CA 90066.
Phone: (310) 397-3404.
Web address: http://www.pirg.org/calpirg.

Privacy Rights Clearinghouse, 5384 Linda Vista Rd.
Suite 306, San Diego, CA 92110. Phone: (619) 298-3396.
Web address: http://www.privacyrights.org.

This publication is a joint project of CALPIRG, Charitable Trust and the Privacy Rights Clearinghouse. It is funded by the San Francisco Foundation's Bank of America Consumer Education Fund.