

Facts and Statistics

A Wall Street Journal poll conducted recently asked Americans what they feared most in the new millennium. Privacy came out on top, substantially higher than terrorism, global warming and overpopulation. A recent Lou Harris poll found that nearly 90% of individuals are concerned about threats to their privacy, an increase from 34% in 1970. The pollster also discovered that 94% of Americans think personal information is vulnerable to misuse; 78% have refused to provide data to a business because they believe the question was too personal.

Their fears are not unfounded. More than ever, the information explosion, aided by an era of easy credit, has led to the expansion of a crime that feeds on the inability of consumers to control who has access to sensitive information and how it is safeguarded. That crime is identity theft.

The Federal Trade Commission has declared identity theft as the fastest growing crime today. More than 700,000 people became victims in 2000 alone.

The facts on identity theft speak for themselves.

- A newly installed FTC hotline (877-IDTHEFT) for reporting identity theft crimes is already logging more than 2,000 calls a week and many people don't yet know of its existence.
- In 1992 TransUnion received only about 35,000 calls about identity theft, from victims and those concerned about potential crime. In 2000, experts estimate that there was between 600,000 to 700,000 victims nationally. This represents an explosive growth in crime numbers, increasing on average 30-40% per year for the past several years.
- The Secret Service estimates that in 1997 consumers lost more than \$745 million due to identity theft.
- Police detectives around the country now estimate that loss to be more than several billion dollars, adding in losses to credit card companies, victim costs including legal assistance, judicial and law enforcement time in investigating and trying cases.
- An independent study in 1999, commissioned by Image Data LLC, an identity theft prevention service, found that approximately one out of every five Americans, or a member of their families, have been victimized by identity theft.
- On average, victims spend 175 hours and \$808 in out-of-pocket expenses to clear their names.

Information sources: Los Angeles Times, the NY Times, Federal Trade Commission, US Secret Service, San Diego Supervisor Dianne Jacob's office, Privacy Rights Clearinghouse.

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. 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 any expenses incurred, in case you are able to request restitution in a later judgment or conviction against the thief. 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 and request a credit report (free to identity theft victims). 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.") Ask how long the fraud alert is posted on your file, 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. Request a free copy of your credit report every few months so you can monitor any new fraudulent activity.

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). *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.)

2. Creditors. Contact all creditors immediately with whom your name has been used fraudulently, by phone and in writing. You may be asked to fill out fraud affidavits. (No law requires these to be notarized at your own expense.) 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" (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.

3. 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. Some police departments don't write reports on such crimes, so be persistent! Also report to the FTC (see end).

4. Stolen checks. If you have had checks stolen or bank accounts set up fraudulently, report it to the appropriate check verification companies (see next page). 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.

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 SSN or your birthdate. Monitor your account statement. You may be liable if fraud is not reported quickly.

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 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)

7. 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/uss)

8. Social Security Number (SSN) misuse. Call Social Security Administration to report fraudulent use of your SSN. As a last resort, you might want to try to change your number, although we don't recommend it except for the most serious cases. The SSA will only change the number if you fit their fraud victim criteria. Also order a copy of your Personal Earnings and Benefits Statement and check it for accuracy. The thief might be using your SSN for employment purposes. (Web: www.ssa.gov)

9. Passports. Whether you have a passport or not, write the passport office to alert them to anyone ordering a passport fraudulently. (Web: travel.state.gov/passport_services.html)

Phone service. If your long distance calling card has been stolen or there are fraudulent charges on the bill, cancel the account and open a new one. Provide a password which must be used any time the account is changed. Pacific Bell fraud hotline: (877) 202-4558.

11. 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. 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: (Calif. DMV) www.dmv.ca.gov/consumer/fraud.htm. Calif. DMV fraud unit, (866) 658-5758. E-mail: dlfraud@dmv.ca.gov. Other states: www.aamva.org/hotlinks.html.

12. 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.

13. 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.

14. 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 to find an attorney who specializes in consumer law, the Fair Credit Reporting Act and the Fair Credit Billing Act.

15. 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. Web: www.idtheftcenter.org

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

17. Don't give in. 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 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. Report such attempts to government regulators immediately.

Resources

Credit reporting bureaus

Equifax: P.O. Box 105069, Atlanta, GA 30348.
Report fraud: Call (800) 525-6285 and write to address above.
Order credit report: (800) 685-1111. Web: www.equifax.com

Experian (formerly TRW): P.O. Box 9532, Allen, TX 75013.
Report fraud: Call (888) EXPERIAN (888-397-3742) and write to address above. Fax: (800) 301-7196.
Order credit report: (888) EXPERIAN.
Web: www.experian.com

Trans Union: P.O. Box 6790, Fullerton, CA 92834.
Report fraud: (800) 680-7289 and write to address above.
Order credit report: (800) 888-4213.
Web: www.transunion.com

To opt out of pre-approved offers of credit for all three bureaus, call (888) 5OPTOUT. 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

Report fraud: (800) 269-0271. Order Earnings & Benefits Statement: (800) 772-1213.
Web: www.ssa.gov

To remove your name from mail and phone lists

Direct Marketing Association (Web: www.the-dma.org)

- 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
- CrossCheck: (800) 843-0760
- 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 help to victims. File your case with the FTC Consumer Response Center, (877) IDTHEFT. Web: 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. Web: www.privacyrights.org.
- **CALPIRG**, 3435 Wilshire Blvd., Suite 380, Los Angeles, CA 90010. (213) 251-3680 or (916) 448-4516. E-mail: calpirg@pirg.org. Web: www.calpirg.org.
- **Identity Theft Resource Center.** Lists local victim support groups: www.idtheftcenter.org. E-mail: voices123@att.net.
- **California Office of Privacy Protection**, (Dept. Of Consumer Affairs), (800) 952-5210. Web: www.privacyprotection.ca.gov.
- **FBI Internet Fraud Complaint Center**, www.ifccfbi.gov
- **U.S. Dept. Of Justice**, identity theft information, www.usdoj.gov/criminal/fraud/idtheft.html
- **Identity Theft Survival Kit.** Phone: (800) 725-0807. Web: www.identitytheft.org.