WHAT DO I NEED TO DO IF I BECOME A VICTIM OF ID THEFT?

STANFORD
RESPONSIBILITY
OWNERSHIP
OPPORTUNITY
TEAMWORK
SOLUTIONS
DIE LUFT DER FREIHEIT WEHT
PUBLIC SAFETY

If Your Identity's Been Stolen

Even if you've been very careful about keeping your personal information to yourself, an identity thief can strike. If you suspect that your personal information has been used to commit fraud or theft, ***take the following four steps right away***. Remember to follow up all calls in writing; send your letter by certified mail, return receipt requested, so you can document what the company received and when; and keep copies for your files.

Place a fraud alert on your credit reports and review your credit reports.

Call the toll-free fraud number of anyone of the three major credit bureaus to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place fraud alerts on your credit report, and all three reports will be sent to you free of charge.

Equifax — To report fraud, call:
1-800-525-6285, and write: P.O. Box 740241, Atlanta, GA 30374-0241

Experian — To report fraud, call:
1-888-EXPERIAN (397-3742), and write: P.O. Box 9532, Allen, TX 75013

TransUnion — To report fraud, call:
1-800-680-7289, and write: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Once you receive your reports, review them carefully. Look for inquiries you didn't initiate, accounts you didn't open, and unexplained debts on your true accounts. You also should check that information such as your SSN, address(es), name or initial, and employers are correct. Inaccuracies in this information also may be due to typographical errors. Nevertheless, whether the inaccuracies are due to fraud or error, you should notify the credit bureau as soon as possible by telephone and in writing. You should continue to check your reports periodically, especially in the first year after you've discovered the theft, to make sure no new fraudulent activity has occurred. The automated "one-call" fraud alert process only works for the initial placement of your fraud alert. Orders for additional credit reports or renewals of your fraud alerts must be made separately at each of the three major credit bureaus.

Close any accounts that have been tampered with or opened fraudulently.

Credit Accounts

Credit accounts include all accounts with banks, credit card companies and other lenders, and phone companies, utilities, ISPs, and other service providers.

If you're closing existing accounts and opening new ones, use new Personal Identification Numbers (PINs) and passwords.

If there are fraudulent charges or debits, ask the company about the following forms for disputing those transactions:

1. For new unauthorized accounts, ask if the company accepts the ID Theft Affidavit (available at www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf).
2. If they don't, ask the representative to send you the company's fraud dispute forms. For your existing accounts, ask the representative to send you the company's fraud dispute forms.
3. If your ATM card has been lost, stolen or otherwise compromised, cancel the card as soon as you can. Get a new card with a new PIN.

Checks

If your checks have been stolen or misused, close the account and ask your bank to notify the appropriate check verification service. While no federal law limits your losses if someone steals your checks and forges your signature, state laws may protect you. Most states hold the bank responsible for losses from a forged check, but they also require you to take reasonable care of your account. For example, you may be held responsible for the forgery if you fail to notify the bank in a timely way that a check was lost or stolen. Contact your state banking or consumer protection agency for more information.

You also should contact these major check verification companies. Ask that retailers who use their databases not accept your checks.

TeleCheck — 1-800-710-9898 or 927-0188

Certegy, Inc. — 1-800-437-5120

International Check Services — 1-800-631-9656

Call SCAN (1-800-262-7771) to find out if the identity thief has been passing bad checks in your name.

File a report with your local police or the police in the community where the identity theft took place.

Keep a copy of the report. You may need it to validate your claims to creditors. If you can't get a copy, at least get the report number.

File a complaint with the FTC.

By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials track down identity thieves and stop them. The FTC also can refer victim complaints to other appropriate government agencies and companies for further action. The FTC enters the information you provide into our secure database.

To file a complaint or to learn more about the FTC's Privacy Policy, visit www.consumer.gov/idtheft. If you don't have access to the Internet, you can call the FTC's Identity Theft Hotline: toll-free 1-877-IDTHEFT (438-4338); TDD: 202-326-2502; or write: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

The FTC works for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit www.ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357).

Stanford University Department of Public Safety

711 Serra St.

Stanford, Ca 94305

(650) 723-9633

http://police.stanford.edu