



Identity Theft



1. Contact the fraud dept of the three major credit bureaus and tell them to flag your file with a fraud alert; ask for a "Fraud Alert/Victim Impact" statement.

- Equifax 1-800-525-6285 www.equifax.com
- Experian 1-800-397-3742 / 888-EXPERIAN www.experian.com
- Trans Union 1-800-916-8800 www.transunion.com
or 1-800-680-7289; Report fraud line: 1-800-680-8800

Order credit report annually and check for errors. Keep copies of your correspondence, phone calls, other documents showing your efforts to correct the problem.

2. Contact Creditors of any accounts that have been tampered with or opened fraudulently.
3. Fill out ID Theft form and forward to applicable agencies.
Download form @ www.consumer.gov/idtheft
Or call the FTC at 877-ID-THEFT
4. File a police report. Get a copy of the report to submit to your creditors and others that may require proof of the crime.
5. Change your PINs and passwords. Close accounts that you know gave been tampered with or opened fraudulently.

Social Security Number Theft

- Contact the Social Security Fraud Hotline at 1-800-269-0271

Additional References

- Federal Trade Commission: www.ftc.com
- Privacy Rights Clearinghouse: www.privacyrights.org

- Beware of con artists who may ask you to “confirm” your enrollment service by disclosing passwords or the credit card account number used to subscribe

Six Ways To Clear Your Good Name

(Listed in Kiplinger's January 2004)

It can take months of phone calls and mountains of paperwork to clean up the mess after an identity theft wrecks your credit. Here's where to start.

File a report with your local police department. “That gives you victim status,” says Tracey Thomas of the Identity Theft Resource Center.

File a complaint with the Federal Trade Commission at 877-382-4357 or www.consumer.gov/idtheft. Use the FTC's ID Theft Affidavit to notify creditors about fraudulent accounts in your name. This spares you the need to complete separate affidavits for each creditor.

Get reports from the major credit bureaus, Equifax (888-766-0008), Experian (888-397-3742) and TransUnion (800-680-7289), and request a fraud alert on your credit file. If you spot accounts that don't belong to you, contact the creditors directly (the credit bureaus should supply phone numbers). Also contact all creditors who have made non-promotional inquiries into your credit file. Such inquiries indicate applications for credit have been made in your name. Send all letters certified mail, return receipt requested.

Contact the fraud departments at the banks, credit-card companies and investment firms at which you have accounts. Ask them to require a PIN or password for all transactions or changes to your accounts. (Avoid using your mother's maiden name or the last four digits of your social security number.)

Get additional help on how to clear your name from the Privacy Rights Clearinghouse (www.privacyrights.org) and the Identity Theft Resource Center (www.idtheftcenter.org).

If necessary, find referrals to lawyers who specialize in Fair Credit Reporting Act issues through the National Association of Consumer Advocates (www.naca.net/resource.htm).

- Public Interest Research Groups: www.pirg.org
- Identity Theft Prevention and Survival: www.identitytheft.org
- Future Crime Prevention Association: www.futurecrime.com
- Internet Fraud Complaint Center: www.ifccfbi.gov

To remove incorrect information from your records, you should contact and follow up with a letter, with each involved:

Credit Bureau; Creditor; Employer; and Government agency

Precautions Against Identity Theft

- Following delivery, promptly remove mail from your mailbox. If going on vacation put a “vacation hold” through the Post Office
- Place outgoing mail in secure mailboxes
- Never provide personal information over the telephone
- Destroy pre-approved credit applications, receipts and bills before discarding
- Do not carry unnecessary credit cards or identification in your wallet or purse
- On an annual basis, order your credit report from the three major credit bureaus
- Never leave receipts at ATMs, bank counters, cash registers, restaurants or public trash receptacles
- Shred all receipts, bills, credit applications, bank statements.
- Do not record personal identification numbers (PINs) or passwords on cards carried in your wallet
- Cut up expired cards immediately
- Be wary of solicitations disguised as promotions offering “instant prizes” designed to obtain personal information
- Be especially protective of personal information when using the internet