

## **If Your Identity's Been Stolen**

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.

### **1. Contact the fraud departments of each of the three major credit bureaus.**

- **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

Tell them you are a victim of identity theft, and ask them to place a “fraud alert” in your file, as well as a “victim statement.” It’s a signal to creditors to call you before they open any new accounts or change your existing accounts, and helps prevent an identity thief from opening additional accounts in your name. At the same time, order copies of your credit reports. Credit bureaus must give you a free copy of your report if it’s inaccurate because of fraud **and** you send them written request.

Check your credit reports carefully to make sure the information is accurate. 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 also may be due to typographical errors. Nevertheless, whether the inaccuracies are due to fraud or error, notify the credit bureau as soon as possible by telephone and in writing. In a few months, order new copies of your reports-both to verify your corrections and changes, and to make sure no new fraudulent activity has occurred.

“Fraud alerts” and “victim statements” are primarily voluntary services of the credit bureaus. Creditors do not have to consider them when granting credit. That’s one more reason to check your credit reports regularly. In addition, fraud alerts and victim statements expire; you need to renew them periodically. Ask each credit bureau about its policy.

### **2. 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:

For new authorized accounts, ask if the company accepts the ID Theft Affidavit (available at [www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf](http://www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf)). 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.

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 financial institution 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.

### **3. File a report with your local police of 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.

### **4. File a complaint with the FTC.**

Visit [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) to file a complaint instantly, obtain a copy of the ID Theft Affidavit and get answers to frequently asked questions about identity theft. If you don't have access to the Internet, call the FTC's Identity Theft Hotline, toll-free, at 1-877-IDTHEFT (438-4338). Your complaint will be entered into a secure consumer fraud database, accessible only to law enforcement agencies, for use in pursuing criminal investigations.