

Identity Theft

Quick Facts

It's important to protect your personal information, and to take certain steps quickly to minimize the potential damage from identity theft if your information is accidentally disclosed or deliberately stolen:

Place a "Fraud Alert" on your credit reports, and review those reports carefully. Notifying one of the three nationwide consumer reporting companies is sufficient.

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

File a police report with local law enforcement officials. This is an essential step in claiming your rights.

Report your theft to the Federal Trade Commission, [online](#), by phone, or by mail.

And before identity theft happens, learn how to safeguard your information at ftc.gov/idtheft.

Identity Theft: What To Do If Your Personal Information Has Been Compromised

The bottom line for online threats like phishing, spyware, and hackers is identity theft. ID theft occurs when someone uses your name, Social Security number, credit card number or other personal information without your permission to commit fraud or other crimes. That's why it's important to protect your personal information. To find out how to deter and detect identity theft, visit ftc.gov/idtheft.

But, according to OnGuard Online, if your personal information is accidentally disclosed or deliberately stolen, taking certain steps quickly can minimize the potential for the theft of your identity.

Place a "Fraud Alert" on your credit reports, and review the reports carefully. The alert tells creditors to follow certain procedures before they open new accounts in your name or make changes to your existing accounts. The three nationwide consumer reporting companies have toll-free numbers for placing an initial 90-day fraud alert; a call to one company is sufficient:

TransUnion: www.transunion.com, 1-800-680-7289

Experian: www.experian.com, 1-888-EXPERIAN (397-3742)

Equifax: www.equifax.com, 1-800-525-6285

Placing a fraud alert entitles you to free copies of your credit reports. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain.

Close accounts. Close any accounts that have been tampered with or established fraudulently:

Call the security or fraud departments of each company where an account was opened or changed without your okay. Follow up in writing, with copies of supporting documents.

Use the [ID Theft Affidavit](#) to support your written statement.

Ask for verification that the disputed account has been closed and the fraudulent debts discharged.

Keep copies of documents and records of your conversations about the theft.

File a police report. File a report with law enforcement officials to help you with creditors who may want proof of the crime. This report will also help you claim your rights as a victim of identity theft.

Report the theft to the Federal Trade Commission. Your report helps law enforcement officials across the country in their investigations.

Online: ftc.gov/idtheft

By phone: 1-877-ID-THEFT (438-4338) or TTY, 1-866-653-4261

How to Report if You Have Been a Victim of Identity Theft

If your information has been misused, file a report about your identity theft with the police, and file a complaint with the Federal Trade Commission at ftc.gov/idtheft. Read [Take Charge: Fighting Back Against Identity Theft](#) for detailed information on other steps to take in the wake of identity theft.

February 2008