

Consumer Alert

Federal Trade Commission ■ Bureau of Consumer Protection ■ Office of Consumer and Business Education

Identity Crisis... What to Do If Your Identity is Stolen

"I don't remember charging those items. I've never even been in that store."

Maybe you never charged those items, but someone else did...someone who used your name and personal information to commit fraud. When an imposter co-opts your name, your Social Security number, your credit card number, or some other piece of your personal information for their use — in short, when someone appropriates your personal information without your knowledge — it's a crime, pure and simple.

The biggest problem? You may not know your identity's been stolen until you notice that something's amiss: you may get bills for a credit card account you never opened, your credit report may include debts you never knew you had, a billing cycle may pass without your receiving a statement, or you may see charges on your bills that you didn't sign for, didn't authorize, and don't know anything about.

First Things First

If someone has stolen your identity, the Federal Trade Commission recommends that you take three actions immediately.

First, **contact the fraud departments of each of the three major credit bureaus.** Tell them to flag your file with a fraud alert including a statement that creditors should call you for permission before they open any new accounts in your name.

	<u>Report fraud</u>	<u>Order credit report</u>	<u>Web site</u>
Equifax:	(800) 525-6285	(800) 685-1111	www.equifax.com
Experian:	(888) EXPERIAN (397-3742)	(888) EXPERIAN	www.experian.com
Trans Union:	(800) 680-7289	(800) 916-8800	www.tuc.com

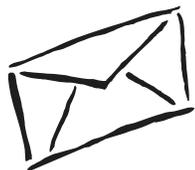
It's a good idea to order a copy of your credit report from the three credit bureaus every year to check on their accuracy and whether they include only those debts and loans you've incurred. This could be very important if you're considering a major purchase, such as a house or a car. A credit bureau may charge you up to \$8 for a copy of your report.

Second, **contact the creditors for any accounts that have been tampered with or opened fraudulently.** Ask to speak with someone in the security or fraud department, and follow up in writing. Following up with a letter is one of the procedures spelled out in the Fair Credit Billing Act for resolving errors on credit billing statements, including charges or electronic fund transfers that you have not made.

Third, **file a police report.** Keep a copy in case your creditors need proof of the crime.

Next, Take Control

Although identity thieves can wreak havoc on your personal finances, there are some things you can do to take control of the situation. Here's how to handle some of the most common forms of identity theft.



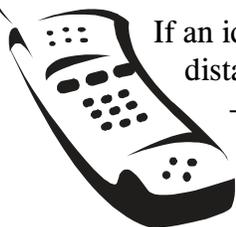
If an identity thief has stolen your mail for access to new credit cards, bank and credit card statements, pre-approved credit offers and tax information or falsified change-of-address forms, (s)he has committed a crime. Report it to your local postal inspector.

If you discover that an identity thief has changed the billing address on an existing credit card account, close the account. When you open a new account, ask that a password be used before any inquiries or changes can be made on the account. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your Social Security number or your phone number, or a series of consecutive numbers. Avoid the same information and numbers when you create a Personal Identification Number (PIN).



To thwart an identity thief who may pick through your trash to capture your personal information, tear or shred your charge receipts, copies of credit applications, insurance forms, bank checks and statements, expired charge cards, and credit offers you get in the mail.

• If you have reason to believe that an identity thief has accessed your bank accounts, checking account or ATM card, close the accounts immediately. When you open new accounts, insist on password-only access. If your checks have been stolen or misused, stop payment. If your ATM card has been lost, stolen or otherwise compromised, cancel the card and get another with a new PIN.



If an identity thief established new phone service in your name and is making long-distance calls, making unauthorized calls that appear to come from — and are billed to — your cellular phone, or using your calling card and PIN, contact your service provider immediately to cancel your account and calling card. Get new accounts and new PINs.

If it appears that someone is using your Social Security number when applying for a job, get in touch with the Social Security Administration to verify the accuracy of your reported earnings and that your name is reported correctly. Call (800) 772-1213 to check your Personal Earnings and Benefit Estimate.

If you suspect that your name or Social Security number is being used by an identity thief to get a driver's license, contact your Department of Motor Vehicles. If your state uses your Social Security number as your driver's license number, ask to substitute another number.

If You're Still Having Identity Problems...

Stay alert to new instances of identity theft. Notify the company or creditor that's involved immediately. Follow up in writing. You also may want to contact:

The Privacy Rights Clearinghouse, which provides information on how to network with other identity theft victims. Call (619) 298-3396 or visit www.privacyrights.org.

The US Secret Service, which has jurisdiction over financial fraud cases. Although the Service generally investigates cases where the dollar loss is substantial, your information may provide evidence of a larger pattern of fraud requiring their involvement. Contact your local field office.

The Social Security Administration, which may issue you a new Social Security number if you still have difficulties even after trying to resolve the problems resulting from identity theft. Unfortunately, there is no guarantee that a new Social Security number will resolve your problems.

Complaint Clearinghouse

The Federal Trade Commission is the federal clearinghouse for consumer complaints about identity theft. The information you provide can help the Commission and other law enforcement agencies track, investigate and prosecute identity thieves.

To file a complaint about identity theft with the Federal Trade Commission, contact the Consumer Response Center by phone: 202-FTC-HELP (382-4357); by TDD: 202-326-2502; by mail: Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580; or by e-mail: use the complaint form at www.ftc.gov.

The FTC publishes brochures on a variety of topics of interest to consumers. For a complete list, ask the CRC for a copy of **Best Sellers** or check it out online at www.ftc.gov.

Chart Your Course of Action

Use this form to record the steps you've taken to report the fraudulent use of your identity.
Keep this list in a safe place for future reference.

Credit Bureaus - Report Fraud

Bureau	Phone Number	Date Contacted	Contact Person	Comments
Equifax	800-525-6285			
Experian	888-397-3742			
Trans Union	800-680-7289			

Bank and Credit Card Account Issuers (Contact each issuer to protect your rights under the Fair Credit Billing Act)

Issuer	Address and Phone Number	Date Contacted	Contact Person	Comments

Law Enforcement Authorities - Report Identity Theft

Agency	Phone Number	Date Contacted	Contact Person	Report Number	Comments