FTC Consumer Alert

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

What To Do If Your Personal Information Has Been Compromised

Companies or institutions that keep personal information about you have an obligation to safeguard it. Still, from time to time, the personal information they hold may be accidentally disclosed or deliberately stolen. If your information falls into the wrong hands, it may be misused to commit fraud against you.

If you get a notice that your personal information may have been compromised, taking certain steps quickly can minimize the potential for the theft of your identity.

If the stolen information includes your financial accounts, close compromised credit card accounts immediately. Consult with your financial institution about whether to close bank or brokerage accounts immediately or first change your passwords and have the institution monitor for possible fraud. Place passwords on any new accounts that you open. Avoid using your mother's maiden name, your birth date, the last four digits of your Social Security number (SSN) or your phone number, or a series of consecutive numbers.

If the stolen information includes your Social Security number, call the toll-free fraud number of any one of the three nationwide consumer reporting companies and place an **initial fraud alert** on your credit reports. This alert can help stop someone from opening new credit accounts in your name.

Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241

Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 2002, Allen, TX 75013

TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

An **initial fraud alert** stays on your credit report for 90 days. When you place this alert on your credit report with one nationwide consumer reporting company, you'll get information about ordering one free credit report from each of the companies. It's prudent to wait about a month after your information was stolen before you order your report. That's because suspicious activity may not show up right away. Once you get your reports, review them for suspicious activity, like inquiries from companies you didn't contact, accounts you didn't open, and debts on your accounts that you can't explain. Check that information — like your SSN, address(es), name or initials, and employers — is correct.

If the stolen information includes your driver's license or other government-issued identification, contact the agencies that issued the documents and follow their procedures to cancel a document and get a replacement. Ask the agency to "flag" your file to keep anyone else from getting a license or another identification document in your name.

Once you've taken these precautions, watch for signs that your information is being misused. For example, you may not get certain bills or other mail on time. Follow up with creditors if your bills don't arrive on time. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover his tracks. Other signs include:

- receiving credit cards that you didn't apply for;
- being denied credit, or being offered less favorable credit terms, like a high interest rate, for no apparent reason; and
- getting calls or letters from debt collectors or businesses about merchandise or services you didn't buy.

Continue to read your financial account statements promptly and carefully, and to monitor your credit reports every few months in the first year of the theft, and once a year thereafter. For more information on getting your credit reports free once a year or buying additional reports, read *Your Access to Free Credit Reports* at http://www.ftc.gov/bcp/conline/pubs/credit/freereports.htm.

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 www.consumer.gov/idtheft. Read *Take Charge: Fighting Back Against Identity Theft* for detailed information on other steps to take in the wake of identity theft.

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); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

FEDERAL TRADE COMMISSION	ftc.gov
1-877-FTC-HELP	FOR THE CONSUMER

March 2005