

IDENTITY THEFT



What You Can Do to Prevent Identity Theft

Check financial statements promptly. Always review your monthly banking, brokerage, and credit card statements for accuracy. Report problems immediately.

Watch your credit. Order copies of your credit report every year from each of the three major credit reporting agencies. They are: Equifax, 800-685-1111, P.O. Box 105851, Atlanta, GA 30348; TransUnion, 800-888-4213, P.O. Box 1000, Chester, PA 19022; and Experian, 888-397-3742, P.O. Box 2002, Allen, TX 75013

Be stingy with information. Never disclose your Social Security number, birth date, or mother's maiden name unless you initiated the transaction. On paper documents, don't include such data unless required to do so on an official application for employment, financing, or insurance. Never put such information on personal Web pages or publicly posted resumes or directories.

Just say no. Consider "opting out" of information-sharing at your financial institutions. (Check your company's financial privacy notice, which is mailed annually and usually posted on company Web sites, to find out how to opt out.) Also opt out of pre-approved credit offers by calling the Credit Reporting Industry Pre-Screening Opt-Out Number at 888-567-8688.

Travel light. Don't carry ID that contains sensitive data like your Social Security number unless absolutely necessary.

Lock it up. Safeguard your driver's license and other government ID at all times. Lock desks, cabinets, and safes containing such information in your office and home.

Shred and destroy. Before throwing out files containing Social Security numbers, account numbers, and birth dates, shred them with a cross-cut shredder. Destroy CDs or floppy disks containing sensitive data.

Guard mail. Consider using a locked mailbox or slot to receive mail at home. Deposit mail in postal mailboxes or in the post office to discourage mail theft.

Beware strange ATMs. Avoid using private or strange-looking automated teller machines, because they may be rigged to skim data off your card's magnetic strip.

No surfing allowed. Watch out for "shoulder surfers" when using pay phones or public internet access; use your free hand to shield the keypad. Don't use cordless phones to conduct sensitive financial or medical business, because eavesdroppers on other phones and those using eavesdropping equipment may be able to overhear your conversations.

Build a wall. Install firewalls and virus detection software on your home computers to discourage hackers.

Log off. Quit your browser and log off after using public internet-access computers in libraries, internet cafes, and the like. If you have a high-speed internet connection at home, unplug the computer's cable or phone line when you are not using it to discourage hackers.

Deal only with reputable Web sites. Check privacy and security policies of Web sites before making purchases, trading stocks, or banking online.

Get complicated. Consider password protecting all your bank and brokerage accounts. Create passwords at least eight characters long.

Check your workplace. Ask how your employer safeguards employee records. Request that Social Security numbers not be used as employee ID numbers.

If You Become a Victim

Report the crime. Filing a report with your local police and keeping a copy yourself will make it easier to prove your case to creditors and merchants and may help you build a lawsuit if you have to sue to recover losses or clear your name later.

File a complaint. The Federal Trade Commission (877-FTC-HELP; TTY, 866-653-4261) investigates interstate and internet fraud. Download a copy of an ID theft affidavit from the FTC's Web site at www.consumer.gov/idtheft to help you notify merchants, financial institutions and credit bureaus. For fraud involving stolen mail, also file a complaint with postal officials at www.usps.com/postalinspectors/fraud/MailFraudComplaint.htm.

Alert credit-reporting agencies. Call TransUnion, Experian, and Equifax to get addresses and instructions. Ask to have your account flagged with a fraud alert.

Notify banks, creditors, and utilities. Close accounts that have been used by thieves. Choose new passwords and PINs for all your accounts and don't use your mother's maiden name as a password.

Order your credit report each year. Get credit reports from all three credit bureaus, and study them closely.

See other help. To share your views about identity theft with your state or federal legislators, visit Consumers Union's public-policy Web site at www.consumersunion.org. For other information, check out the nonprofit identity Theft Resource Center at www.idtheftcenter.or and the Privacy Rights Clearinghouse at www.privacyrights.org.