

LifeLock Identity Theft Protection Tips

- **Assume they already have it.** You've already given your personal information to all of your doctors, dentists, employers, health care providers and the list goes on. More than 90,000 Americans are notified daily that their information has been lost or stolen. Protect your credit today by placing a fraud alert with the three major credit bureaus: Experian, Equifax and TransUnion.
- **Alert yourself.** Set a fraud alert with the three major credit bureaus. These "red flags" are designed to alert you to anyone – including yourself – that is opening new lines of credit or making changes to existing lines of credit in your name. Be alert to the fact that these fraud alerts will expire after 90 days. Set a reminder to yourself to renew.
- **Check financial statements promptly.** Always review your monthly banking, brokerage, and credit-card statements for accuracy. If you own a home, check with your mortgage holder on a regular basis to ensure your home equity line-of-credit has not had any fraudulent activity. 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, 800-997-2493; TransUnion, 800-888-4213; and Experian, 888-397-3742. Report errors promptly and in writing. To order your annual free credit report, go to www.annualcreditreport.com.
- **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. (Ask employers, schools, and financial institutions to offer alternatives.) Never put such information on personal Web pages or publicly posted résumés 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.) Also opt out of pre-approved credit offers by calling the Credit Reporting Industry Pre-Screening Opt-Out Number at 1-888-5-OPTOUT (888-567-8688).
- **Travel light.** Don't carry identification that contains sensitive data like your Social Security number unless absolutely necessary.
- **Lock it up.** Safeguard your driver's license and other government identification 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 by shredding, cutting, or breaking them. Use hard-drive shredding

software or remove and destroy your hard drive before discarding a computer. Just deleting files isn't enough.

- **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.
- **Keep your eye on the prize.** Try not to let waiters, sales clerks, or gas-station attendants disappear from view with your credit or debit card, to avoid "skimming." Crooks can use a handheld card reader to copy the information from your card's magnetic strip.
- **Beware of 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. Six- or seven-character PINs (personal identification numbers) are harder to crack than shorter ones, but you may not be able to use them at machines abroad.
- **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. Don't pay bills, bank, or conduct other financial transactions on public computers. 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. A professional-looking Web site is no guarantee of security. Don't respond to unsolicited e-mail requests for personal information.
- **Hide yourself.** Be cautious of the information you post on online social networks.
- **Shop smart.** When shopping online check to make sure the site you are on is secure before entering any payment information.
- **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.

- **Get involved.** If you are interested in asking Congress to pass stronger financial privacy protections, visit consumersunion.org and click on "Campaigns."
- **Stay alert.** Watch out for scams via email, text message or phone calls. "Phishing," "smishing" and "vishing" are often used by criminals to trick you into giving out personal information. Even if a message seems legitimate, always contact the institution yourself using a phone number or web address you know to be valid.
- **Do more.** If your personal information is breached by a company, do not rely on credit monitoring services as a solution. These services only alert you once you already have a problem and do nothing to keep a thief from using your information.
- **Remember your children.** Call the major credit bureaus – Experian, Equifax and TransUnion – and check quarterly for a credit report for your child. You want to be certain that no credit report exists. Check with the Social Security Administration on an annual basis to ensure that your child does not have a work history. And, most importantly, avoid giving out their personal information as much as possible, always ask what the information is needed for and how it will be safeguarded.

