

TAKE THESE STEPS TO REDUCE YOUR RISK OF BECOMING A VICTIM OF IDENTITY THEFT

Criminals can commit identity theft relatively easily because of lax credit industry practices, careless information-handling practices in the workplace, and the ease of obtaining SSNs. But you can reduce your risk of fraud by following certain tips. **The most important advice we can give you is to check your credit report at least once a year.**

CREDIT CARDS, DEBIT CARDS, AND CREDIT REPORTS:

1. Reduce the number of credit and debit cards you carry in your wallet. We recommend that you do not use debit cards because of the potential for losses to your checking account (see above). Instead, carry one or two credit cards and your ATM card in your wallet. Nonetheless, debit cards are popular. If you do use them, take advantage of online access to your bank account to monitor account activity frequently. Report evidence of fraud to your financial institution immediately.
2. Do not use debit cards when shopping online. Use a credit card because you are better protected—in case of fraud.
3. Keep a list or photocopy of all your credit cards, debit cards, bank accounts, and investments—the account numbers, expiration dates and telephone numbers of the customer service and fraud departments—in a secure place (not your wallet or purse) so you can quickly contact these companies in case your credit cards have been stolen or accounts are being used fraudulently.
4. Never give out your SSN, credit or debit card number or other personal information over the phone, by mail, or on the Internet unless you have a trusted business relationship with the company and **you** have initiated the call. Identity thieves have been known to call their victims with a fake story that goes something like this. "Today is your lucky day! You have been chosen by the Publishers Consolidated Sweepstakes to receive a free trip to the Bahamas. All we need is your Social Security number, credit card number and expiration date to verify you as the lucky winner."
5. Order your credit report at least once a year. Federal law gives you the right to one free credit report each year from the three credit bureaus: Equifax, Experian, and TransUnion. If you are a victim of identity theft, your credit report will contain the tell-tale signs – inquiries that were not generated by you, as well as credit accounts that you did not open. The earlier you detect fraud, the easier and quicker it will be to clean up your credit files and regain your financial health.

How to order your free annual credit report:

- By telephone: (877) 322-8228
- Online: www.annualcreditreport.com
- By mail. Print out the order form here: <https://www.annualcreditreport.com/cra/requestformfinal.pdf>

PASSWORDS AND PINS:

6. When creating passwords and PINs (personal identification numbers), do not use the last four digits of your Social Security number, mother's maiden name, your birthdate, middle name, pet's name, consecutive numbers or anything else that could easily be discovered by thieves. It's best to create passwords that combine letters and numbers.
7. Memorize all your passwords. Don't record them on anything in your wallet.

SOCIAL SECURITY NUMBERS:

8. Protect your Social Security number. Release it only when absolutely necessary (like tax forms, employment records, most banking, stock and property transactions). Your SSN is the key to your credit and banking accounts and is the prime target of criminals.

COMPUTER AND INTERNET ACCESS:

9. Anyone using a computer connected to the Internet should install basic protective technology: firewall and antivirus software. While these two solutions aren't a substitute for common-sense behavior, they can help protect against some malicious programs floating about out there. It's also a good idea to invest in encryption software—especially to protect information on things that can be easily lost or stolen, like your laptop, smartphone, or PDA.

TAKE THESE STEPS IF YOU HAVE BECOME A VICTIM OF IDENTITY THEFT:

- 1. Notify credit bureaus.** Immediately report the situation to the fraud department of the three credit reporting companies: Experian, Equifax, and TransUnion.

Equifax: Report fraud:	Experian: Report fraud:	TransUnion: Report fraud: Call
Call (888) 766-0008 and write to address above. TDD: (800) 255-0056 Web: www.equifax.com	Call (888) EXPERIAN (888-397-3742) and write to address above. TDD: Use relay to fraud number above. Web: www.experian.com/fraud	(800) 680-7289 and write to address above. TDD: (877) 553-7803 Web: www.transunion.com

Once you have received your three credit reports, examine each one carefully. Report fraudulent accounts and erroneous information in writing to both the credit bureaus *and* the credit issuers following the instructions provided with the credit reports. The FTC's identity theft guide provides a sample letter to send to the credit bureaus requesting that fraudulent accounts be blocked.

Once you notify the credit bureaus about the fraudulent accounts, the bureau is required to block that information from future reports. The bureau must also notify the credit grantor of the fraudulent account.

- 2. Law enforcement.** Report the crime to your local police or sheriff's department right away. You might also need to report it to police department(s) where the crime occurred if it's somewhere other than where you live. Give them as much documented evidence as possible. *Make sure the police report lists the fraudulent accounts. Get a copy of the report, which is called an "identity theft report" under the FCRA.* Keep the phone number of your investigator handy and give it to creditors and others who require verification of your case. Credit card companies and banks may require you to show the report in order to verify the crime.
- 3. What to do with new credit accounts opened by the imposter.** If your credit report shows that the imposter has opened new accounts in your name, contact those creditors immediately by telephone and in writing. Recent amendments to the FCRA (§623(6)(B)) allow you to prevent businesses from reporting fraudulent accounts to the credit bureaus.
- 4. ATM cards.** If your ATM or debit card has been stolen or compromised, report it immediately. Contact your bank and fill out a fraud affidavit. Get a new card, account number, and password. Do not use your old password. Closely monitor your account statements. You may be liable if the fraud is not reported quickly. Start with a phone call and immediately follow up in writing. Read the debit card contract for information about liability. Some cards are better protected in cases of fraud than others.
- 5. Brokerage accounts.** You do not have the same protections against loss with brokerage accounts as you do with credit and debit card or bank accounts. The Securities Investor Protection Corporation (www.sipc.org) restores customer funds only when a brokerage firm fails. If an identity thief or other fraudster targets your brokerage account, refer to your account agreement for information on what to do. Immediately report the incident to the brokerage company and notify the Securities and Exchange Commission, www.sec.gov also notify the National Association of Securities Dealers, www.nasd.org. To protect against fraud, put a password on each of your investment accounts. For more on identity theft involving brokerage accounts, how it can happen, and what to do, see the PRC alert, www.privacyrights.org/ar/BrokerageAlert.htm
- 6. Legal help.** You may want to consult an attorney to determine legal action to take against creditors, credit bureaus, and/or debt collectors if they are not cooperative in removing fraudulent entries from your credit report or if negligence is a factor. Call the local Bar Association (www.abanet.org/premartindale.html), a Legal Aid office in your area (for low-income households), or the National Association of Consumer Advocates (www.naca.net) to find an attorney who specializes in consumer law, the Fair Credit Reporting Act, and the Fair Credit Billing Act.

If you are a senior citizen or take care of a dependent adult, be sure to contact an elder law service or the nearest Aging and Independent Services program. Many district attorneys have an elder abuse unit with expertise in financial crimes against seniors.

Lenox Advisors. Integrating financial security into financial success.

Learn more at www.lenoxadvisors.com