

Identity Fraud

A CONSUMER'S TOP 10 TIPS TO PREVENT IDENTITY FRAUD

Traditional shopping

1. Review your wallet or purse contents before you go shopping. Common theft is the easiest way for a criminal to steal your identity and commit fraud. Before you go shopping, think about how much information a thief would obtain if your wallet or purse was stolen.

- Avoid carrying Social Security cards, birth certificates or passports unless absolutely necessary.
- Don't carry extra credit cards unless you plan to use them.

2. Create a list of all your credit card and bank account information and store in a secure place.

- Be sure to include account numbers, expiration dates and credit limits. Also include the telephone numbers or emails or the customer service and fraud departments.
- If you find your card missing or stolen, refer to this list and immediately notify your credit card provider of the loss. This not only prevents fraudulent charges, but it also notifies your provider if the card is used again.

3. Protect your passwords and PIN numbers.

- When creating passwords and PINs, do not use the last four digits of your Social Security number, mother's maiden name, your birth date, 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.
- Ask your financial institutions to add extra security protection to your account. Most will allow you to use an additional code or password (a number or word) when accessing your account. If asked to create a reminder question, do not use one that is easily answered by others.
- Memorize all your passwords. Don't record them on anything in your wallet.

4. Review your credit report now. One of the easiest ways to see if a criminal is fraudulently using your identity is to review your credit report.

- Be sure to report mistakes to the credit bureaus. A federal law gives consumers the right to receive one free copy of their credit report every 12 months from each of the three main credit bureaus (Experian, Equifax, TransUnion).



- Order a report today from one bureau and review it, looking for discrepancies. In four months, order another report from a second bureau. In another four months, order a report from the third bureau. Doing this will enable you to see snapshots of your credit throughout the year at no cost.

5. Never provide confidential information over the phone to an unsolicited caller claiming that they represent a financial institution or creditor. Criminals often will use your Social Security number to open up fraudulent accounts or gain access to financial information or assets.

- Do not have your Social Security number printed on your checks and do not allow merchants to write your Social Security number on your checks.
- If a business requests your Social Security number, ask them why they need it. If it is not a valid reason, don't provide it.
- If you receive an unsolicited call and are asked to provide information, get the caller's name, location, telephone number, and reason that they are calling. Call them back at the phone number on your billing statements to verify the caller's identification.

6. Never put outgoing checks or bill payments in your home mailbox, as they are easy to steal. While sending checks is a popular and desired holiday gift, it also has its risks, as thieves can steal mail containing checks and gain other personal information from bills and financial statements.

- Where practical, drop all items containing checks or financial information in a secure postal mailbox or at the post office.

Online shopping

7. Log off completely when finished with online transactions.

Closing or minimizing your browser or typing a new Web address may not be enough to prevent others from accessing your online information.

- Instead, click “log off” to terminate your online session. In addition, don’t allow your browser to “remember” your username and password information.

8. Increase your own computer’s security.

Personal firewalls and security software packages (with anti-virus, anti-spam and spyware detection features) are a must-have for those who plan on shopping online.

- Make sure your computer has the latest security patches, and make sure that you access your online financial accounts only on a secure Web page using encryption.

9. Avoid emailing personal and financial information.

Although your computer may be “well protected” with proper firewall, antivirus, Internet security or encryption software, the individual or company receiving your information may not have similar security in place.

- Always confirm with online retailers that they have proper Internet security in place before responding to any email request.

10. Delete, without replying to, any suspicious email requests.

Hackers and spammers often impersonate retailers to lure personal financial information.

- If there is any reason to doubt the authenticity of an email message from a company you do business with, don’t click on links or buttons in the message. Instead, type the Internet address of the company into your browser, log on as you usually do, and examine your account information. You may also telephone a company to ask if an email is legitimate.

Travelers knows identity fraud.

To learn more, talk to your independent agent or visit travelersbond.com.



travelersbond.com

Travelers Casualty and Surety Company of America and its property casualty affiliates. One Tower Square, Hartford, CT 06183

This material does not amend, or otherwise affect, the provisions or coverages of any insurance policy or bond issued by Travelers. It is not a representation that coverage does or does not exist for any particular claim or loss under any such policy or bond. Coverage depends on the facts and circumstances involved in the claim or loss, all applicable policy or bond provisions, and any applicable law. Availability of coverage referenced in this document can depend on underwriting qualifications and state regulations.

© 2013 The Travelers Indemnity Company. All rights reserved. Travelers and the Travelers Umbrella logo are registered trademarks of The Travelers Indemnity Company in the U.S. and other countries. 59592 Rev. 10-13