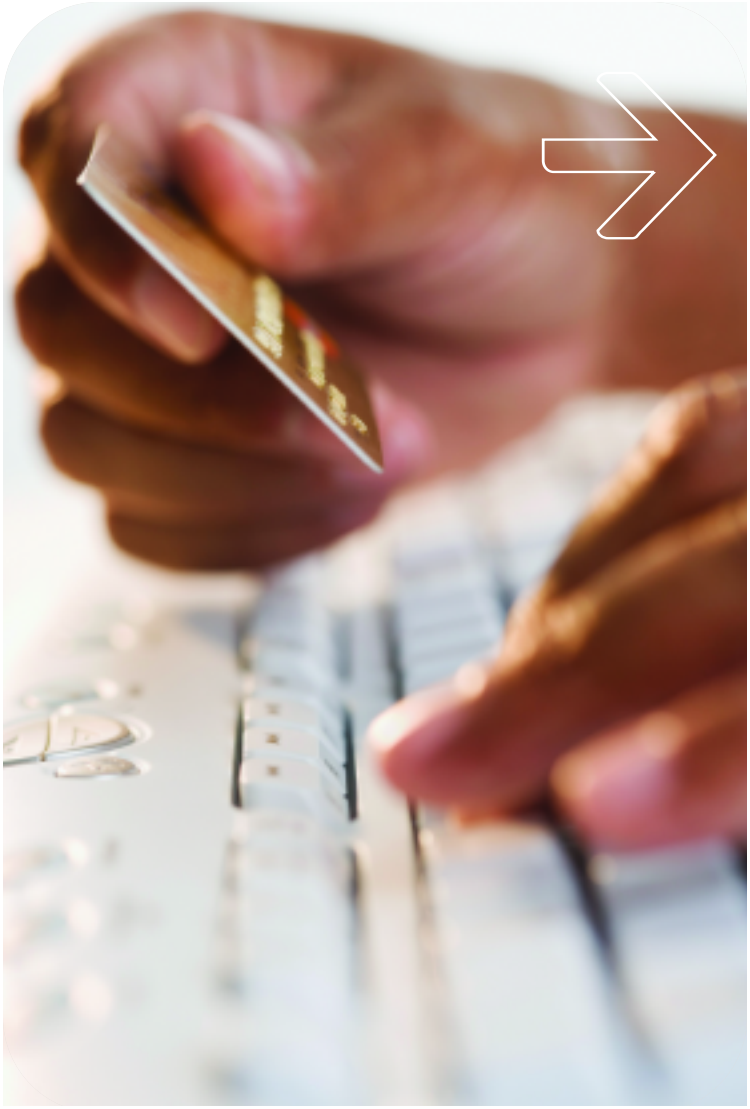
Protect yourself.

STEPS TO TAKE TO AVOID IDENTITY THEFT IN THE FUTURE

TRAVELERS
Insurance. In-synch.℠



Becoming a victim of identity theft is a frightening and frustrating experience. It can happen to anyone at any time. Our recovery guide can help you during this difficult time.

What you should do today

- 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. Do not contact the bureaus directly for this free report. Instead, TransUnion, Experian or Equifax reports are available by logging on to www.annualcreditreport.com, by calling 877.322.8228 or by writing to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Order a report today from one bureau and review it. Four months from now, order another report from a second bureau. Four months after that order a report from the third bureau. Doing this will enable you to see snapshots of your credit throughout the year at no cost.
- Review your wallet or purse contents. If lost or stolen, how much information will a thief obtain? Don't carry Social Security cards, birth certificates or passports with you unless absolutely necessary. Don't carry extra credit cards. If you carry a health care card, look to see if your Social Security number is being used as your ID number. If it is, ask if it can be changed.
- Create a list or make a photocopy of all your credit cards and bank account information along with their account numbers, expiration dates and credit limits, as well as the telephone numbers of customer service and fraud departments. Store this list in a safe place.
- Reduce the number of pre-approved credit card offers you receive by calling 888.5.OPTOUT (your Social Security number is required). This removes your name from the marketing lists of all three credit bureaus.
- To reduce telemarketing calls, register with the Federal Trade Commission's National Do Not Call Registry at www.donotcall.gov or by phone at 888.382.1222.
- Send a postcard with your name, address and signature to the Direct Marketing Association's Mail Preference Service at P.O. Box 643, Carmel, NY 10512. The Association does not sell marketing lists but its member companies can check the list and voluntarily remove names.
- Check your Social Security Statement of your earnings and benefits once each year to make sure that no one else is using your Social Security number for employment. Visit www.ssa.gov/mystatement/ to request a copy.
- If you are on active duty in the military, put an active duty alert on your credit files. The alert will stay in your files for at least 12 months. If someone applies for credit in your name, the creditors will take extra precautions to make sure that the applicant is not someone pretending to be you.
  - Equifax, 800.525.6285, TDD 800.255.0056, www.equifax.com;
  - Experian, 888.397.3742, TDD 800.972.0322, www.experian.com;
  - TransUnion, 800.680.7289, TDD 877.553.7803, www.transunion.com.
- Take the identity theft quiz at www.idsafety.net or www.onguardonline.gov/quiz.

What you should do every day

- Guard your Social Security number. 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, use an alternate number.
- Never put outgoing checks, bill payments or tax documents in your home mailbox, as they are easy to steal. Drop all items in a postal mailbox or at the post office.
- Know your billing cycles, and watch for any missing mail. Follow up with creditors if bills or new cards do not arrive on time. An identity thief may have filed a change of address request in your name with the creditor or the post office.
- Bring in your mail daily. Do not leave mail in your mailbox. If you will be away from home and unable to get your mail, have the post office hold it for you. You can make this request online at www.usps.com.
- When you order new checks, ask when you can expect delivery. If your mailbox is not secure, ask to pick up the checks at your bank instead of having them delivered to your home.
- Never give out confidential information (e.g., account numbers, passwords) over the phone to an unsolicited caller claiming that they represent your financial institution or a creditor. Get their name, location, telephone number, and reason that they are calling. Call them back at the phone number on your billing statements.
- Be alert to red flags. If you receive a call from a merchant, creditor or collection agency in what seems to be a case of mistaken identity, be on alert. Find out exactly who they are and details of why they are calling. This may be your first and only warning that you are a victim of identity fraud.

- Carefully consider what information you want placed in the residence telephone book and ask yourself what it reveals about you. Consider having your telephone number unlisted or list your number but without your address.
- Going through people's garbage is a common way for criminals to get information about you. Destroy charge receipts, copies of credit applications, insurance forms, bank checks and statements, expired charge cards and credit offers you get in the mail. Keep track of credit card, debit card and ATM receipts. Never dispose of receipts in a public trash container. Bring them home and shred them when you no longer need them.
- When you fill out a loan or credit application, be sure that the business either shreds these applications or stores them in locked files.
- Carefully review your monthly account statements and bills (including credit card statements, bank statements, utility bills and cell phone bills) for unauthorized charges as soon as you receive them. If you suspect unauthorized use, contact the provider's customer service and fraud departments immediately.
- Use passwords and PINs that are difficult to guess for all accounts and change them periodically.
- Sign your credit cards immediately upon receipt. Clearly write "Check ID" next to your signature.
- When possible, use credit cards that have your photo and signature on the front.
- Take precautions to prevent strangers from overhearing your conversations.
- Watch out for people standing near you at retail stores, restaurants, grocery stores, etc., that have a cell phone in hand. With camera phones, they can take a picture of your credit card to obtain your name, number, and expiration date.
- When possible, watch your credit card as the merchant completes the transaction.
- Ask businesses what their privacy policies are and how they will use your information. Can you choose to keep it confidential? Do they restrict access to data?
- If you are denied credit or employment, find out why. It could be due to errors on your credit report.
- Visit www.ftc.gov for more information.

What you should do online

- Delete, without replying to, any suspicious email requests.
- 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. If not, make sure the organization being impersonated is aware of the scam and alert the Anti-Phishing Working Group at reportphishing@antiphishing.org, the FTC at uce@ftc.gov and the FBI's Internet Crime Complaint Center at www.ic3.gov.
- Avoid emailing personal and financial information.

What you should do online (continued)

- Don't trust email headers, as they can be forged easily.
- Avoid filling out forms in email messages. You can't know with certainty where the data will be sent, how it will be used or who will use it.
- Be wary of email messages asking you to verify or re-enter account information that you have already given to an organization. Don't provide confidential information, like a PIN for an ATM card. Think twice before entering credit card numbers for offers that appear too good to be true.
- If you get an email that warns you, with little or no notice, that an account of yours will be shut down unless you reconfirm your billing information, do not reply or click on the link in the email. Instead, contact the company cited in the email using a telephone number or Web site address you know to be genuine.
- Use extra caution with wireless Internet connections. Wireless networks may not provide as much security as wired Internet connections. In fact, many "hotspots" – wireless networks in public areas like airports, hotels and restaurants – reduce their security so it's easier for individuals to access and use these networks. You can learn more about security issues relating to wireless networks on the Web site of the Wi-Fi Alliance (www.wi-fi.org).
- Beef up your security. Personal firewalls and security software packages (with anti-virus, anti-spam, and spyware detection features) are a must-have for those who engage in online financial transactions. 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.
- Even if a Web page starts with "https" and contains a key or closed padlock symbol in the bottom right corner of the window, it's still possible that it may not be secure. Some criminals, for example, make spoofed Web sites which appear to have padlocks. To double-check, click on the padlock icon on the status bar to see the security certificate for the site. Follow the "Issued to" link in the pop-up window. You should see the name matching the site you think you're on. If the name differs, you are probably on a spoofed site.
- Log off completely when finished with online transactions or checking online accounts. Closing or minimizing your browser or typing in a new Web address when you're done using your online account may not be enough to prevent others from gaining access to your online information. Instead, click on the "log off" button to terminate your online session. In addition, you shouldn't permit your browser to "remember" your username and password information.
- Be careful what you download. When you download a program or file from an unknown source, you risk loading malicious software programs on your computer. Fraudsters often hide these programs within seemingly benign applications. Think twice before you click on a pop-up advertisement or download a "free" game or gadget.

- Report suspicious activity to the FTC. Forward any suspicious messages to uce@ftc.gov. If you believe you've been scammed, file a complaint at www.ftc.gov, and visit the FTC's ID Theft Web site (www.ftc.gov/idtheft) to learn how to minimize your risk of damage from identity theft.
- Use your own computer. It's generally safer to access your online accounts from your own computer than from other computers. If you use a computer other than your own, for example, you won't know if it contains viruses or spyware. If you do use another computer, be sure to delete all of your "Temporary Internet Files" and clear all of your "History" after you log off your account.
- Visit www.onguardonline.gov for more valuable information.

TRAVELERS

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

travelers.com