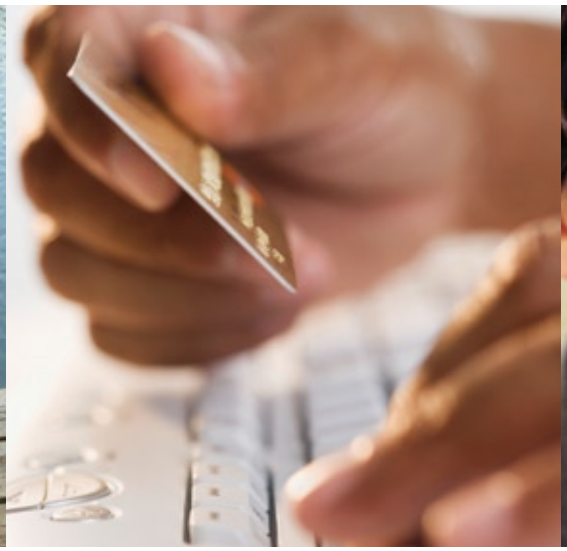
The complete guide to identity theft recovery.



Get back to your life.

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.

Start by reviewing and completing the Identity Theft Affidavit. The step-by-step process shown on the Affidavit will guide you to fix your credit and resolve your problems. Remember to use the Contact Tracking Worksheet whenever you make a telephone call or send a letter.

The Affidavit and Worksheet will describe how to use the sample letters provided.

AFFADAVIT AND CONTACT TRACKING WORKSHEET

Be sure to read the Statement of Victim's Rights and the tips for protecting yourself.

Travelers will be there for you. Our dedicated Identity Fraud Claim Team can provide expert advice that is in-synch with your needs. If you have questions about the documents in this kit please call our claims office at **800.842.8496.**

Instructions for Completing the ID Theft Affidavit

To make certain that you do not become responsible for any debts incurred by an identity thief, you must prove to each of the companies where accounts were opened or used in your name that you didn't create the debt.

A group of credit grantors, consumer advocates, and attorneys at the Federal Trade Commission (FTC) developed an ID Theft Affidavit to make it easier for fraud victims to report information. While many companies accept this affidavit, others require that you submit more or different forms. Before you send the affidavit, contact each company to find out if they accept it.

It will be necessary to provide the information in this affidavit anywhere a **new** account was opened in your name. The information will enable the companies to investigate the fraud and decide the outcome of your claim. If someone made unauthorized charges to an **existing** account, call the company for instructions.

This affidavit has two parts:

- Part One — the ID Theft Affidavit — is where you report general information about yourself and the theft.

- Part Two — the Fraudulent Account Statement — is where you describe the fraudulent account(s) opened in your name. Use a separate Fraudulent Account Statement for each company you need to write to.

When you send the affidavit to the companies, attach copies (NOT originals) of any supporting documents (for example, driver's license or police report). Before submitting your affidavit, review the disputed account(s) with family members or friends who may have information about the account(s) or access to them.

Complete this affidavit as soon as possible. Many creditors ask that you send it within two weeks. Delays on your part could slow the investigation.

Be as accurate and complete as possible. You may choose not to provide some of the information requested. However, incorrect or incomplete information will slow the process of investigating your claim and absolving the debt. Print clearly.

When you have finished completing the affidavit, mail a copy to each creditor, bank, or company that provided the thief with the unauthorized credit, goods, or services you describe. Attach a copy of the Fraudulent Account Statement with information only on accounts opened at the institution to which you are sending the packet, as well as any other supporting documentation you are able to provide.

Send the appropriate documents to each company by certified mail, return receipt requested, so you can prove that it was received. The companies will review your claim and send you a written response telling you the outcome of their investigation. Keep a copy of everything you submit.

If you are unable to complete the affidavit, a legal guardian or someone with power of attorney may complete it for you. Except as noted, the information you provide will be used only by the company to process your affidavit, investigate the events you report, and help stop further fraud. If this affidavit is requested in a lawsuit, the company might have to provide it to the requesting party. Completing this affidavit does not guarantee that the identity thief will be prosecuted or that the debt will be cleared.

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

If you haven't already done so, report the fraud to the following organizations:

1. Any one of the nationwide consumer reporting companies to place a fraud alert on your credit report. Fraud alerts can help prevent an identity thief from opening any more accounts in your name. The company you call is required to contact the other two, which will place an alert on their versions of your report, too.

   - **Equifax:** 1-800-525-6285; www.equifax.com
   - **Experian:** 1-888-EXPERIAN; (397-3742); www.experian.com
   - **TransUnion:** 1-800-680-7289; www.transunion.com

In addition to placing the fraud alert, the three consumer reporting companies will send you free copies of your credit reports, and, if you ask, they will display only the last four digits of your Social Security number on your credit reports.

2. The security or fraud department of each company where you know, or believe, accounts have been tampered with or opened fraudulently. Close the accounts. Follow up in writing, and include copies (NOT originals) of supporting documents. It's important to notify credit card companies and banks in writing. Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures.

   When you open new accounts, use new Personal Identification Numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your Social Security number or your phone number, or a series of consecutive numbers.

3. Your local police or the police in the community where the identity theft took place to file a report. Get a copy of the police report or, at the very least, the number of the report. It can help you deal with creditors who need proof of the crime. If the police are reluctant to take your report, ask to file a "Miscellaneous Incidents" report, or try another jurisdiction, like your state police. You also can check with your state Attorney General's office to find out if state law requires the police to take reports for identity theft. Check the Blue Pages of your telephone directory for the phone number or check www.naag.org for a list of state Attorneys General.

4. The Federal Trade Commission. By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them. The FTC also can refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws that the FTC enforces.

   You can file a complaint online at **www.consumer.gov/idtheft.** If you don't have Internet access, call the FTC's Identity Theft Hotline, toll-free: 1-877-IDTHEFT (438-4338); TTY: 1-866-653-4261; or write: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

ID Theft Affidavit

VICTIM INFORMATION

(1) My full legal name is _____
(First) (Middle) (Last) (Jr., Sr., III)

(2) (If different from above) When the events described in this affidavit took place, I was known as

_____
(First) (Middle) (Last) (Jr., Sr., III)

(3) My date of birth is _____
(day/month/year)

(4) My Social Security number is _____

(5) My driver's license or identification card state and number are _____

(6) My current address is _____
City _____ State _____ ZIP Code _____

(7) I have lived at this address since _____
(month/year)

(8) (If different from above) When the events described in this affidavit took place, my address was

_____
City _____ State _____ ZIP Code _____

(9) I lived at the address in Item 8 from _____ until _____
(month/year) (month/year)

(10) My daytime telephone number is ( ) _____

My evening telephone number is ( ) _____

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

HOW THE FRAUD OCCURRED

Check all that apply for items 11 - 17:

(11) ☐ I did not authorize anyone to use my name or personal information to seek the money, credit, loans, goods or services described in this report.

(12) ☐ I did not receive any benefit, money, goods or services as a result of the events described in this report.

(13) ☐ My identification documents (for example, credit cards; birth certificate; driver's license; Social Security card; etc.) were

☐ stolen ☐ lost on or about _____.
(day/month/year)

(14) ☐ To the best of my knowledge and belief, the following person(s) used my information (for example, my name, address, date of birth, existing account numbers, Social Security number, mother's maiden name, etc.) or identification documents to get money, credit, loans, goods or services without my knowledge or authorization:

Name (if known)	Name (if known)
Address (if known)	Address (if known)
Phone number(s) (if known)	Phone number(s) (if known)
Additional information (if known)	Additional information (if known)

(15) ☐ I do NOT know who used my information or identification documents to get money, credit, loans, goods or services without my knowledge or authorization.

(16) ☐ Additional comments: (For example, description of the fraud, which documents or information were used or how the identity thief gained access to your information.)

(Attach additional pages as necessary.)

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

VICTIM'S LAW ENFORCEMENT ACTIONS

(17) (check one) I ☐ am ☐ am not willing to assist in the prosecution of the person(s) who committed this fraud.

(18) (check one) I ☐ am ☐ am not authorizing the release of this information to law enforcement for the purpose of assisting them in the investigation and prosecution of the person(s) who committed this fraud.

(19) (check all that apply) I ☐ have ☐ have not reported the events described in this affidavit to the police or other law enforcement agency. The police ☐ did ☐ did not write a report. *In the event you have contacted the police or other law enforcement agency, please complete the following:*

(Agency #1)	(Officer/Agency personnel taking report)
(Date of report)	(Report number, if any)
(Phone number)	(email address, if any)
(Agency #2)	(Officer/Agency personnel taking report)
(Date of report)	(Report number, if any)
(Phone number)	(email address, if any)

DOCUMENTATION CHECKLIST

Please indicate the supporting documentation you are able to provide to the companies you plan to notify. Attach copies (NOT originals) to the affidavit before sending it to the companies.

(20) ☐ A copy of a valid government-issued photo-identification card (for example, your driver's license, state-issued ID card or your passport). If you are under 16 and don't have a photo-ID, you may submit a copy of your birth certificate or a copy of your official school records showing your enrollment and place of residence.

(21) ☐ Proof of residency during the time the disputed bill occurred, the loan was made or the other event took place (for example, a rental/lease agreement in your name, a copy of a utility bill or a copy of an insurance bill).

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

(22) ☐ A copy of the report you filed with the police or sheriff's department. If you are unable to obtain a report or report number from the police, please indicate that in Item 19. Some companies only need the report number, not a copy of the report. You may want to check with each company.

SIGNATURE

I certify that, to the best of my knowledge and belief, all the information on and attached to this affidavit is true, correct, and complete and made in good faith. I also understand that this affidavit or the information it contains may be made available to federal, state, and/or local law enforcement agencies for such action within their jurisdiction as they deem appropriate. I understand that knowingly making any false or fraudulent statement or representation to the government may constitute a violation of 18 U.S.C. §1001 or other federal, state, or local criminal statutes, and may result in imposition of a fine or imprisonment or both.

_____ _____

(signature) (date signed)

_____

(Notary)

[Check with each company. Creditors sometimes require notarization. If they do not, please have one witness (non-relative) sign below that you completed and signed this affidavit.]

Witness:

_____ _____

(signature) (printed name)

_____ _____

(date) (telephone number)

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

Fraudulent Account Statement

Completing this Statement

- Make as many copies of this page as you need. **Complete a separate page for each company you're notifying and only send it to that company.** Include a copy of your signed affidavit.
- List only the account(s) you're disputing with the company receiving this form. **See the example below**.
- If a collection agency sent you a statement, letter or notice about the fraudulent account, attach a copy of that document (**NOT** the original).

I declare (check all that apply):

☐ As a result of the event(s) described in the ID Theft Affidavit, the following account(s) was/were opened at your company in my name without my knowledge, permission or authorization using my personal information or identifying documents:

Creditor Name/Address *(the company that opened the account or provided the goods or services)*	**Account Number**	**Type of unauthorized credit/goods/services provided by creditor** *(if known)*	**Date issued or opened** *(if known)*	**Amount/Value provided** *(the amount charged or the cost of the goods/services)*
Example Example National Bank 22 Main Street Columbus, Ohio 22722	01234567-89	auto loan	01/05/2002	$25,500.00

☐ During the time of the accounts described above, I had the following account open with your company:

Billing name _____

Billing address _____

Account number _____

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

TRAVELERS

IDENTITY FRAUD CONTACT TRACKING WORKSHEET

Use this tracking worksheet to document communications you have regarding your identiy theft case. Also included here are helpful tips and other contact resources.

Tips For Organizing Your Case

Accurate and complete records will help you to resolve your identity theft case more quickly.

- Have a plan when you contact a company. Don't assume that the person you talk to will give you all of the information or help that you need. Prepare a list of questions to ask the representative about your identity theft. Don't end the call until you are sure you understand everything you have been told. If you need more help, ask for a supervisor.
- Write down the name of everyone you talk to on this Contact Tracking Worksheet. Write down what he or she tells you and the date of the conversation.
- Follow up in writing with all contacts you make on the telephone or in person. Use certified mail and return receipt to document what the organization received and when.
- Make copies of all correspondence or forms you send.
- Keep the originals of supporting documents, like police reports and letters to and from creditors; send copies only.
- Set up a filing system for easy access to your paperwork.
- Keep old files even if you believe your case is closed. Once resolved, most cases stay resolved, but problems can crop up.
- For more detailed information visit www.ftc.gov.

Contact the Fraud Departments at the Three Major Credit Bureaus

Explain that you are a victim of identity theft, and request that a fraud alert be placed in your file, as well as a fraud victim's statement, which asks creditors to call you before opening any new accounts or making changes to your existing accounts. Be sure to leave a daytime and evening phone number where you can be reached. Also, ask for a free copy of your credit report. Order new copies in a few months to verify that corrections were made and to make sure no new fraudulent activity has occurred. As a victim, you should always ask for free reports. (See sample letters provided in the Travelers recovery guide.)

Bureau	Telephone Number	Date Contacted	Person Contacted	Comments
Equifax	800.525.6285			
Experian	888.397.3742			
TransUnion	800.680.7289			

Contact Your Creditors and Financial Institutions

Promptly contact the fraud department at each of your creditors, including banks, credit card issuers, phone and utility companies, and other lenders. To protect your legal rights, follow-up with a letter to each. (See sample letter provided in the Travelers recovery guide.) Write to creditors at the address given for "billing inquiries," NOT the address for sending your payments. Check for fraudulent charges and/or changes-of-address on all your accounts. Close any accounts that have been compromised and close any accounts that are not yours. Be sure to use different, non-obvious Personal Identification Numbers (PINs) and passwords. Ask that inquiries related to fraud be removed. If your ATM/debit card has been lost, stolen or otherwise compromised, cancel the card as soon as possible.

Creditor Address and Phone #	Date Contacted	Person Contacted	Comments

File a Police Report and Contact the Federal Trade Commission

Be sure to file a police report with both your local police and the police department in the community where the theft took place. Get a copy of the report(s) to use as proof of the crime when dealing with creditors. Also file a complaint with the FTC at the number below or via their online ID theft form at: http://www.consumer.gov/idtheft/.

Complaints are entered into a secure consumer fraud database, accessible only to law enforcement agencies, for use in pursuing criminal investigations.

Agency/Department	Telephone Number	Date Contacted	Person Contacted	Report Number Assigned & Comments
Federal Trade Commission	877.IDTHEFT (877.438.4338)			
Local Police				
Police Where Crime Occurred				

Stop Payment on Stolen Checks

If your checks have been stolen or misused, contact your bank immediately to obtain stop payment instructions. Also contact the major check verification companies below to request that they notify retailers using their databases not to accept these checks. (See generic sample letter provided in the Travelers recovery guide.)

Institution	Telephone Number	Date Contacted	Person Contacted	Comments
(Bank Name)				
Certegy, Inc.	800.437.5120			
Global Payments	800.638.4600			
TeleCheck	800.710.9898			
SCAN	800.262.7771			

Other Potential Needs of ID Theft Victims

Issue	Contact
Remove fraudulent phone charges (in your state)	State Public Utility Commission
Remove fraudulent long distance or cell phone charges	888.CALL.FCC (888.225.5322)
Report fraudulent use of your Social Security number. The Social Security Administration (SSA) does not work on financial identity theft cases. SSA only gets involved through the Office of Inspector General if there is benefit fraud or theft of benefit checks.	800.269.0271. We have also included a sample letter to the Social Security Administration in this kit. See sample letters in the Travelers recovery guide.
Report fraudulent use of your SSN to obtain a driver's license	State Department of Motor Vehicles (www.onlinedmv.com). Speak to a fraud investigator.
Report mail theft that resulted in fraudulent accounts opened in your name	U.S. Postal Inspector (not the local post office manager) (www.usps.gov/websites/depart/inspect) or use your local telephone directory.

Other Contacts

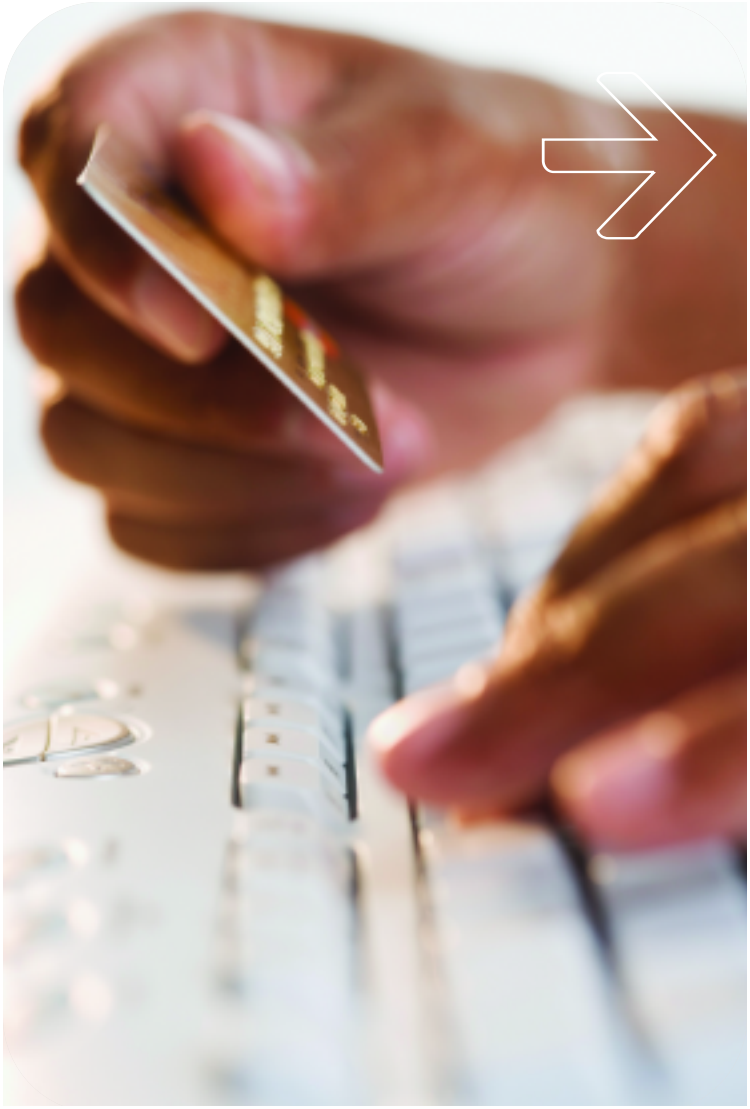
Use this space to record contact with any group or organization not listed in the tables above. (See generic sample letter provided in the Travelers recovery guide.)

Organization	Telephone Number	Date Contacted	Person Contacted	Comments

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.

This kit contains the following:

- Identity theft affidavit
- Contact tracking worksheet
- Statement of victim's rights
- Sample letters that can be sent to credit bureaus, financial institutions, creditors and government agencies
- Claim forms for proof of loss and wage verification
- Tips for protecting yourself in the future

TRAVELERS

Insurance. In-synch.℠

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

Your rights

The Fair Credit Reporting Act (FCRA) gives you rights when you are, or believe you are, the victim of identity theft:

- You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft. A consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number.
- You have the right to free copies of the information in your files at each of the three nationwide agencies (your "file disclosure"). See www.ftc.gov/credit.
- If you believe information in your file results from identity theft, you have the right to ask that a consumer reporting agency block that information from your file.
- You have the right to obtain documents relating to fraudulent transactions made and to accounts opened using your personal information. See www.consumer.gov/idtheft.
- You also may prevent businesses from reporting information about you to consumer reporting agencies if you believe the information is a result of identity theft.

SAMPLE LETTERS AND CLAIM FORMS

- You have the right to obtain detailed information from a debt collector such as late notices or account statements. If you ask, a debt collector must provide you with certain information about the debt you believe was incurred in your name by an identity thief – like the name of the creditor and the amount of the debt. By law, if you inform a collector that a debt resulted from identity theft, that collector must inform the creditor. Creditors are then prohibited from selling such debt or placing them for collection. See www.consumer.gov/idtheft.
- You have the right to have a police report taken. Many states do not have an express law about this but if you are persistent you should be able to get a report in the jurisdiction where you live. With a police report you are entitled to:
  - A seven year fraud alert instead of the 90-day alert
  - A credit freeze in states that have passed that legislation – see www.ncsl.org and search for "credit freeze"
  - Have inaccurate or fraudulent information blocked from your credit report
  - Receive a copy of all application and transaction records on accounts opened fraudulently in your name

LETTER TO EXPERIAN

Date: _____

From: Name: _____

Address: _____

_____

Phone: _____

Email: _____

To: Experian
Attention: Fraud Department
Post Office Box 9532
Allen, TX 75012

Re: Notification of Fraudulent Activities

Dear Sir or Madam:

I am writing to inform you of fraudulent activities in my credit file. On _____ (fill in date) I learned that I may be the victim of an identity theft. The following information relates to transactions which may appear on my credit report that I have not made and therefore requires your attention. (Consumer, please check all boxes that apply.)

☐ Please place a fraud alert on my account and alert me of any activity.

☐ The following account(s) and transaction(s) was/were fraudulently opened/performed in my name.

_____

☐ The address you have on file for me is incorrect. Please refer to the correct address at the top of this page and change your records accordingly.

☐ The following fraudulent transactions on my account were resolved with the creditor/financial institution. Please confirm that the fraudulent transactions have been corrected on my account.

_____

☐ Other: _____

Enclosed you will find documentation supporting my contention. Please respond to me in writing with an update on the progress of your own investigation or action taken within 30 days of your receipt of this notification. Please also send me an updated credit report.

If you require more information, or if you have any questions, please contact me in writing at the address referenced above. Thank you for your time and attention with this matter.

Yours truly,

_____
(signature)

Enclosures: _____

LETTER TO EQUIFAX

Date: _____

From: Name: _____

Address: _____

_____

Phone: _____

Email: _____

To: Equifax
Attention: Fraud Department
Post Office Box 105069
Atlanta, GA 30348

Re: Notification of Fraudulent Activities on Account Number _____

Dear Sir or Madam:

I am writing to inform you of fraudulent activities in my credit file. On _____ (fill in date) I learned that I may be the victim of an identity theft. The following information which may appear on my credit report does not relate to any transaction that I have made and therefore requires your attention. (Consumer, please check all boxes that apply.)

☐ Please place a fraud alert on my account and alert me of any activity.

☐ The following account(s) and transaction(s) was/were fraudulently opened/performed in my name.

_____

☐ The address you have on file for me is incorrect. Please refer to the correct address at the top of this page and change your records accordingly.

☐ The following fraudulent transactions on my account were resolved with the creditor/financial institution. Please confirm that the fraudulent transactions have been corrected on my account.

_____

☐ Other: _____

Enclosed you will find documentation supporting my contention. Please respond to me in writing with an update on the progress of your own investigation or action taken within 30 days of your receipt of this notification. Please also send me an updated credit report.

If you require more information, or if you have any questions, please contact me in writing at the address referenced above. Thank you for your time and attention with this matter.

Yours truly,

_____
(signature)

Enclosures: _____

LETTER TO CREDITOR / FINANCIAL INSTITUTION

Date: _____

From: Name: _____

Address: _____

_____

Phone: _____

Email: _____

To: Creditor/Financial Institution Name: _____

Attention: Complaint Department/Fraud Department

Address: _____

_____

Re: Notification of Fraudulent Activities on Account Number _____

Dear Sir or Madam:

I am writing to inform you of fraudulent activities in my credit file. On _____ (fill in date) I learned that I may be the victim of an identity theft. The following information which may appear on my credit report does not relate to any transaction that I have made and therefore requires your attention. (Consumer, please check all boxes that apply.)

☐ Please place a fraud alert on my account and alert me of any activity.

☐ The following account(s) was/were fraudulently opened in my name. Please close the referenced account(s).

_____

☐ My address was fraudulently changed. Please refer to the correct address at the top of this page and change your records accordingly.

☐ My checks were stolen or lost. Please close the account number referenced above, open a new account in my name and issue new checks.

☐ My credit/debit card was stolen or lost. Please deactivate the card and close the account.

☐ In addition, there are charges on my account which I did not make. I have highlighted the fraudulent charges on the attached statement(s). Please remove these charges as well as any finance or other charges related to the fraudulent activity from my account. Upon completion, please alert the credit reporting agencies that these charges were false.

☐ My phone card/service was fraudulently used. have highlighted the calls on the statement(s) attached. Please remove these charges from my account.

☐ I would like this account to only be accessible with a password. Please provide me with an appropriate contact and instructions on how to have a password activated.

☐ Other: _____

Enclosed you will find documentation supporting my contention. Please respond to me, in writing, with an update on the progress of your own investigation or action taken within 30 days of your receipt of this notification. Please also send me a corrected statement of my account.

If you require more information, or if you have any questions, please contact me in writing at the address referenced above. Thank you for your time and attention with this matter.

Yours truly,

_____

(signature)

Enclosures: _____

Date: _____

From: Name: _____

Address: _____

_____

Phone: _____

Email: _____

To: Company Name: _____

Attention: Complaint/Fraud Department

Address: _____

_____

Re: Notification of Fraudulent Activities

Dear Sir or Madam:

I am writing to inform you that I recently became the victim of an identity theft. This information does not relate to any transaction that I have made. On _____ (consumer, please fill in date and check all boxes that apply):

☐ The following account(s) was/were fraudulently opened in my name. Please close the referenced account(s) and contact the mechant(s) (if applicable).

_____

_____

_____

☐ My address was fraudulently changed. Please refer to the correct address at the top of this page and change your records accordingly.

☐ Other:

_____

_____

_____

Enclosed you will find documentation supporting my contention. Please respond to me in writing with an update on the progress of your own investigation or action taken within 30 days of your receipt of this notification.

If you require more information, or if you have any questions, please contact me in writing at the address referenced above. Thank you for your time and attention with this matter.

Yours truly,

_____

(signature)

Enclosures: _____

LETTER TO SOCIAL SECURITY

Date: _____

From: Name: _____

Address: _____

_____

Phone: _____

Email: _____

To: Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION
P. O. Box 17768
Baltimore, MD 21235

Re: Notification of Fraudulent Activities

Dear Sir or Madam:

I am writing to inform you that I recently became the victim of an identity theft. On _____ (consumer, please fill in date and check all boxes that apply):

☐ My Social Security number may have been stolen. Please provide me with a Social Security Statement and change your records to note the correct address shown at the top of this page.

☐ My address was fraudulently changed. Please refer to the correct address at the top of this page and change your records accordingly.

☐ My passport may have been fraudulently used. Please investigate and advise me of any action I need to take.

☐ A judgment has been wrongly entered in my name for actions taken or debt incurred by an identity thief. Please investigate and advise me of any action I need to take.

☐ Other: _____

Enclosed you will find documentation supporting my contention. Please respond to me in writing with an update on the progress of your own investigation or action taken within 30 days of your receipt of this notification.

If you require more information, or if you have any questions, please contact me in writing at the address referenced above. Thank you for your time and attention with this matter.

Yours truly,

_____
(signature)

Enclosures: _____

LETTER TO TRANSUNION

Date: _____

From: Name: _____

Address: _____

_____

Phone: _____

Email: _____

To: TransUnion
Attention: Fraud Department
Post Office Box 6790
Fullerton, CA 92834

Re: Notification of Fraudulent Activities

Dear Sir or Madam:

I am writing to inform you of fraudulent activities in my credit file. On _____ (fill in date) I learned that I may be the victim of an identity theft. The following information relates to transactions which may appear on my credit report that I have not made and therefore require your attention. (Consumer, please check all boxes that apply.)

☐ Please place a fraud alert on my account and alert me of any activity.

☐ The following account(s) and transaction(s) was/were fraudulently opened/performed in my name.

_____

☐ The address you have on file for me is incorrect. Please refer to the correct address at the top of this page and change your records accordingly.

☐ The following fraudulent transactions on my account were resolved with the creditor/financial institution. Please confirm that the fraudulent transactions have been corrected on my account.

_____

☐ Other: _____

_____

Enclosed you will find documentation supporting my contention. Please respond to me, in writing, with an update on the progress of your own investigation or action taken within 30 days of your receipt of this notification. Please also send me an updated credit report.

If you require more information, or if you have any questions, please contact me in writing at the address referenced above. Thank you for your time and attention with this matter.

Yours truly,

_____
(signature)

Enclosures: _____

TRAVELERS

PROOF OF LOSS

NOTE
Furnishing of Proof of Loss forms is without prejudice. All rights and defenses are reserved and the conditions of the POLICY are not waived. Where needed additional pages should be used to provide the requested information and receipts or other documents to substantiate claimed amounts should be attached to this form.

Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information, or conceals for the purpose of misleading, information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime, and may also be subject to a civil penalty. (In New York, the civil penalty is not to exceed five thousand dollars and the stated value of the claim for each such violation. In Colorado, any insurance company or agent of an insurance company who knowingly provides false, incomplete, or misleading facts or information to a policyholder or claimant for the purpose of defrauding or attempting to defraud the policyholder or claimant with regard to a settlement or award payable from insurance proceeds shall be reported to the Colorado Division of Insurance within the Department of Regulatory Agencies.)

IDENTITY FRAUD EXPENSE COVERAGE CLAIM

POLICY NO.	INSURED PERSON:	CLAIM NUMBER:

THIS AFFIDAVIT IS EXECUTED BY

_____ in the following capacity:

[X] Insured person, or legal representative thereof, under the above-captioned policy.

WHO HEREBY ATTESTS TO THE FOLLOWING:

1. This loss is due to: (check appropriate box and attach documentary evidence which supports and explains the loss)

   ☐ Expenses incurred and paid by the Insured as a direct result of any one **Identity Fraud** (as defined under the policy):

   ☐ Lost wages as a result of time taken off from work to meet with, or talk to law enforcement agencies, credit agencies and/or legal counsel, or to complete fraud affidavits, as the direct result of an **Identity Fraud**.

2. Location of loss	Date Insured learned of loss	Date loss reported to Travelers

3. Describe how Insured discovered the loss

_____

_____

_____

4. Social Security Number:	In processing my claim for **Identity Fraud**, I understand and authorize Travelers and any other affiliated company to obtain a credit report(s) and/or a consumer report(s) from a consumer reporting agency to verify and obtain information regarding my claim. ☐ Check here if you would like to receive a copy of the consumer report(s) or credit report(s).

POLICY:	INSURED PERSON:

5. The loss in the amount of $_____, and is set forth in the following itemized statement (attached documentary evidence which supports and explains any one or more of the items):

ATTACHMENT	DESCRIPTION	AMOUNT		TOTAL	
	Total Claimed at this time: →				
	Less Deductible: →				
	Amount Claimed: →				
	(Attach additional sheets if further space is needed)				

2. I have no other **Identity Fraud** insurance coverage except:

_____

_____

_____

DATE	SIGNATURE
DATE SUBSCRIBED AND SWORN	NOTARY PUBLIC

TRAVELERS

WAGE AND SALARY VERIFICATION FORM

Employer Name and Address

_____

_____

_____

_____

Employee Name and Address

_____

_____

_____

_____

Social Security No. _____

1-5 to be completed by employer regarding employee named above:

1. Occupation: _____

2. Dates of employment: FROM _____ THROUGH _____

3. Wage or salary as of date of loss: PER HOUR $ _____ PER WEEK $ _____ PER MONTH $ _____

   NO. HOURS WORKED _____ PER DAY _____ PER WEEK _____ PER MONTH _____

   NO. DAYS WORKED _____ PER WEEK _____

4. Dates absent due to identity fraud:

   FROM _____ THROUGH _____

   OR INDIVIDUAL DATES AS FOLLOWS: _____

   _____

   _____

5. Dates absent for other reasons: FROM _____ THROUGH _____

6. If you are self-employed, please attach your tax return for the period(s) and any other documentation that supports your claim for loss.

Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information, or conceals for the purpose of misleading, information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime, and may also be subject to a civil penalty. (In New York, the civil penalty is not to exceed five thousand dollars and the stated value of the claim for each such violation. In Colorado, any insurance company or agent of an insurance company who knowingly provides false, incomplete, or misleading facts or information to a policyholder or claimant for the purpose of defrauding or attempting to defraud the policyholder or claimant with regard to a settlement or award payable from insurance proceeds shall be reported to the Colorado Division of Insurance within the Department of Regulatory Agencies.)

Employee authorization – The undersigned hereby authorizes release of the above information:

Date: _____ Signed: _____

Telephone: (_____) _____

Signature of employer: _____

Signature: _____

Printed name and title: _____

Date: _____

Your Identity Fraud Expense Reimbursement Coverage

The identity fraud coverage from Travelers is designed to reimburse you for the out-of-pocket expenses described in your policy form. These are the expenses related to cleaning up your credit if you have been victimized. In general, the coverage will reimburse identity theft victims for the following:

- Lost wages as a result of time taken off from work to deal with the fraud, including wrongful incarceration
- Notary and certified mail charges for completing and delivering fraud affidavits
- Fees to re-apply for loans that were denied as a result of erroneous credit information due to the identity theft
- Long distance telephone charges for calling merchants, law enforcement agencies or credit grantors to discuss an actual identity theft
- Attorney fees incurred, with Travelers Bond's prior consent, for:
  - Defending suits brought incorrectly by merchants or their collection agencies
  - Removing criminal or civil judgments wrongly entered against the victim
  - Challenging information in a credit report

Please review your policy form for specific coverage details. If you have any questions about your coverage please contact the Travelers Bond Identity Fraud Claim Team at 800.842.8496

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

The Travelers Indemnity Company
and its property casualty affiliates
One Tower Square
Hartford, CT 06183

travelers.com