

Identity Crisis ...

What to Do If Your Identity is Stolen





DEPARTMENT OF POLICE



A Nationally Accredited
Police Agency

***“I don’t remember opening that credit card account
And certainly didn’t buy those items I’m being billed for.”***

Maybe you never opened that account, but someone else did... someone who used your name and personal information to commit fraud. When-an imposter co-opts your name, your Social Security Number (SSN), your credit card number, or some other piece of your personal information for their use — in short, when someone appropriates your personal information without your knowledge — it’s a crime, pure and simple

The biggest problem? You may not know your identity’s been stolen until you notice that something’s amiss: you may get bills for a credit card account you never opened, your credit report may include debts you never knew you had, a billing cycle may pass without your receiving a statement, or you may see charges on your bills that you didn’t sign for, didn’t authorize, and don’t know anything about.

First Things First

If someone has stolen your identity, the Federal Trade Commission recommends that you take three actions immediately.

First, contact the fraud departments of each of the three major credit bureaus. Tell them to flag your file with a fraud alert including a statement that creditors should get your permission before opening any new accounts in your name.

At the same time, ask the credit bureaus for copies of your credit reports. Credit bureaus must give you a free copy of your report if it is inaccurate because of fraud Review your reports carefully to make sure no additional fraudulent accounts have been opened in your name or unauthorized changes made to your existing accounts. In a few months, order new copies of your reports to verify your corrections and changes, and to make sure no new fraudulent activity has occurred.

Order Credit Report

Equifax 800-685-1111
Experian 888-397-3742
Trans Union 800-916-8800

Report Fraud Web Site

800-525-6285 www.equifax.com
888-397-3742 www.experian.com
800-680-7289 www.tuc.com



Second, contact the creditors for any accounts that have been tampered with or opened fraudulently. Ask to speak with someone in the security or fraud department, and follow up in writing. Following up with a letter is one of the procedures spelled out in the Fair Credit Billing Act for resolving errors on credit billing statements, including charges that you have not made.

Third, file a report with your local police or the police in the community where the identity theft took place. Keep a copy in case your creditors need proof of the crime.

Next, Take Control

Although identity thieves can wreak havoc on your personal finances, there are some things you can do to take control of the situation. Here's how to handle some of the most common forms of identity theft.

If an identity thief has stolen your mail for access to new credit cards, bank and credit card statements, pre-approved credit offers and tax information or falsified change-of-address forms, (s)he has committed a crime. Report it to your local postal inspector.

If you discover that an identity thief has changed the billing address On an existing credit card account, close the account. When you open a new account, ask that a password be used before any inquiries or changes can be made on the account. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers. Avoid the same information and numbers when you create a Personal Identification Number (PIN).



If you have reason to believe that 'an identity thief has accessed your bank accounts, checking account or ATM card, close the accounts immediately. When you open new accounts, insist on password-only access. If your checks have been stolen or misused, stop payment. If your ATM card has been lost, stolen, or otherwise compromised, cancel the card and get another with new PIN.



If an identity thief has established new phone or wireless service in your name and is making unauthorized calls that appear to come from — and are billed to — your cellular phone, or is using your calling card and PIN, contact your service provider immediately to cancel the account and calling card. Get new accounts and new PINs.

If it appears that someone is using your SSN when applying for a job, get in touch with the Social Security Administration (SSA) to verify the accuracy of your reported earnings and that your name is reported correctly. Call (800) 772-1213 to check your Social Security statement.

In addition, the SSA may issue you a new SSN at your request if, after trying to resolve the problems brought on by identity theft, you continue to experience problems. Consider this option carefully. A new SSN may not resolve your identity theft problems, and may actually create new problems. For example, a new SSN does not necessarily ensure a new credit record because credit bureaus may combine the credit records from your old SSN with those from your new SSN. Even when the old credit information is not associated with your new SSN, the absence of any credit history under your new SSN may make it more difficult for you to get credit. And finally, there's no guarantee that a new SSN wouldn't also be misused by an identity thief.

If you suspect that your name or SSN is being used by an identity thief to get a driver's license, report it to your Department of Motor Vehicles. Also, if your state uses your SSN as your driver's license number, ask to substitute another number.

Stay Alert

Taking the steps outlined here should, in most cases, resolve your identity theft problems, but identity theft or related credit problems may reoccur. Stay alert to new instances of identity theft. Notify the company or creditor that's involved immediately. Follow up in writing.

Order a copy of your credit report from the three credit bureaus every year to check on their accuracy and whether they include only those debts and loans you've incurred. This could be very important if you're considering a major purchase, such as a house or a car. A credit bureau may charge you up to \$8.50 for a copy of your report.

Complaint Clearinghouse

If you've been a victim of identity theft, file a complaint with the FTC by contacting the FTC's Identity Theft Hotline by telephone: toll-free 1-877-IDTHEFT (438-4338); TDD: 202-326-2502; by mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580; or online: www.consumer.gov/idtheft. Ask for a copy of *ID Theft: When Bad Things Happen to Your Good Name*, a free comprehensive consumer guide to help you guard against and recover from identity theft.

Privacy: What You Do Know Can Protect You

Our economy generates an enormous amount of data. Most users of that information are from honest businesses — getting and giving legitimate information. Despite the benefits of the information age, some consumers may want to limit the amount of personal information they share. And they can:

More organizations are offering people choices about how their personal information is used. For example, many feature an “opt-out” choice that limits the information shared with others or used for promotional purposes. When you “opt-out,” you may cut down on the number of unsolicited telemarketing calls, promotional mail and spam e-mails that you receive. Learn more about the options you have for protecting your personal information by contacting the following organizations.

Credit Bureaus

The credit bureaus offer a toll-free number to call to “opt-out” of having pre-approved credit offers sent to you for two years. Call 1-888-5-OPTOUT (567-8688) for more information. (See **Attached Form – Page 13**)

Department of Motor Vehicles

The Drivers Privacy Protection Act forbids states from distributing personal information to direct marketers. It allows sharing of personal information with law enforcement officials, courts, government agencies, private investigators, insurance underwriters and similar businesses. Check with your state DMV to learn more, or visit www.ftc.gov/privacy/protect.htm#Motor

Direct Marketers

The Direct Marketing Association offers the Mail and Telephone Preference Services, which allow you to opt out of receiving direct mail marketing and telemarketing calls from many national companies for five years.

When you register with these services, your name will be put on a “delete” file that is updated four times a year and made available to direct-mail and telephone marketers. Two to three months after your name is entered into the quarterly file, you should notice a decrease in the number of solicitations you receive. However, your registration will not stop mailings or calls from organizations not registered with the DMA’s Mail and Telephone Preference Services.

To have your name deleted from many direct mail or telemarketing lists, write your own letter or use the sample letter. Mail it to the following addresses:

For direct mail marketing:

Direct Marketing Association
Mail Preference Service
P.O. Box 9008
Farmingdale, NY 11735-9008

OR

Preference Service Manager
Direct Marketing Association
1120 Avenue of the Americas
New York, NY 10036-6700.

Or go online at <http://www.the-dma.org/consumers/offmailinglist.html>

For telemarketing:

Direct Marketing Association
Telephone Preference Service
P0 Box 9014
Farmingdale, NY 11735-9014

OR

Preference Service Manager
Direct Marketing Association
1120 Avenue of the Americas
New York, NY 10036-6700

Or fax to: 212-790-1427; or go online at: <http://www.the-dma.org/consumers/offtelephonestlist.html>

In addition, some states maintain their own “Do Not Call” lists. For more information visit [http:// www.the-dma.org/governmentldonotcallist&shtml](http://www.the-dma.org/governmentldonotcallist&shtml)

For E-mail:

The DMA recently launched a new EMail Preference Service to help you reduce unsolicited commercial emails. To “opt-out” of receiving unsolicited commercial email, use the Direct Marketing Association’s online form at www.e-mps.org. Your online request will remain effective for one year.

For More Information

To learn more about more about privacy issues and how they affect your life and the decisions you may make in the marketplace, visit www.consumer.gov/ncpw.

The FTC works for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them. To file a complaint or to get free information on consumer issues, call toll-free, 1-877-FTC-HELP (382-4357), or use the complaint form at www.ftc.gov. The FTC enters Internet, telemarketing, identity theft and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Instructions for Completing the ID Theft Affidavit

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

A working group composed of credit grantors, consumer advocates and the Federal Trade Commission (FTC) developed this 1D Theft Affidavit to help you report information to many companies using just one standard form. Use of this affidavit is optional. 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.

You can use this affidavit where 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 to find out what to do.)

This affidavit has two parts: **(See Attached Forms - Pages 8-12)**

- **ID Theft Affidavit** is where you report general information about yourself and the theft.
- **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 (e.g., drivers license, police report) you have.

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 of receiving it. Delaying 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. Please 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 to each affidavit a copy of the Fraudulent Account Statement with information only on accounts opened at the institution receiving 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 for your records.

If you cannot 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.

Use this page to record information about your personal financial records, like your credit card account numbers and toll-free customer service lines; your savings and checking accounts and the branch that holds your accounts; the name, phone number and address of your lawyer; your Social Security Number; your health and life insurance policies; where important papers are kept, such as your will, deed to your house, and title to your car. Keep this information in a safe place. Make sure someone you trust knows about this list in case of emergency.

To learn more about household record keeping, check out the following materials:

Keeping Family/Household Records

http://www.pueblo.gsa.gov/cic_text/money/keeprecords/keeprecords.htm

Where to Write for Vital Records

http://www.pueblo.gsa.gov/cic_text/misc/vital-records/w2welcom.htm

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 #8 from _____ until _____
(month/year) (month/year)
- (10) My daytime telephone number is (____) _____
My evening telephone number is (____) _____

Check all that apply for items 11-22:

- (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 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)

Address (if known)

Phone number(s) (if known)

Additional information (if known)

Name (if known)

Address (if known)

Phone number(s) (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.)

Victim's Law Enforcement Actions

- (17) I am I am not willing to assist in the prosecution of the person(s) who committed this fraud.
- (18) I am I 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) I have I 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)

(E-Mail Address, if any)

(Agency #2)

(Officer/Agency personnel taking a report)

(Date of Report)

(Report Number, if any)

(Phone Number)

(E-Mail 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).

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 <small>(the company that opened the account or provided the goods or services)</small>	Account Number	Type of Unauthorized Credit/Goods/Services Provided by Creditor <small>(if known)</small>	Date Issued or Opened <small>(if known)</small>	Amount/Value Provided <small>(the amount charged or the cost of the goods/services)</small>
Example Example National Bank 22 Main Street Columbus, Ohio 22722	01234567-89	Auto Loan	01/05/2003	\$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: _____

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

1. Each of the three national consumer reporting agencies. Ask each agency to place a "fraud alert on your credit report, and send you a copy of your credit file. When you have completed your affidavit packet, you may want to send them a copy to help them investigate the disputed accounts.
 - ◆ **Equifax Credit information Services, Inc.** (800) 525-6285 (Hearing impaired call 1-800-255-0056 and ask the operator to call the Auto Disclosure Line at 1-800-685-1111 to obtain a copy of your report.) P.O. Box 740241, Atlanta, GA 30374-0241 www.equifax.com
 - ◆ **Experian Information Solutions, Inc.**
(888) 397-3742/ TDD (800) 972-0322
P.O. Box 9530, Allen, TX 75013
www.experian.com
 - ◆ **TransUnion**
(800) 680-7289/TDD (877) 553-7803
Fraud Victim Assistance Division
P.O. Box 6790, Fullerton, CA 92634-6790 www.transunion.com
2. The fraud department at each creditor, bank, or utility/service that provided the identity thief with unauthorized credit, goods or services. This would be a good time to find out if the company accepts this affidavit, and whether they require notarization or a copy of the police report.
3. Your local police department. Ask the officer to take a report and give you the report number or a copy of the report. When you have completed the affidavit packet, you may want to give your police department a copy to help them add to their report and verify the crime.
4. The FTC, which maintains the Identity Theft Data Clearinghouse — the federal government's centralized identity theft complaint database — and provides information to identity theft victims. You can call toll-free I-877-ID-THEFT (1-877-438-4338), visit www.consumer.gov/idtheft, or send mail to:

Identity Theft Data Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

The FTC collects complaints from identity theft victims and shares their information with law enforcement nationwide. This information also may be shared with other government agencies, consumer reporting agencies, and companies where the fraud was perpetrated to help resolve identity theft related problems.

Credit Bureaus: Sample Opt-Out Letter

Be sure to send your letter to ALL three credit bureaus:

Options

Equifax, Inc.
P.O. Box 740123
Atlanta, GA 30374-0123

Experian

Consumer Opt-Out
701 Experian Parkway
Allen, TX 75013

TransUnion Corporation's

Name Removal Option
P.O. Box 97328
Jackson, MS 39288-7328

Date

To whom it may concern:

Please remove my name from your marketing lists. Here is the information you have asked me to include:

FIRST, MIDDLE & LAST NAME

(List all name variations, including Jr., Sr., etc.)

CURRENT MAILING ADDRESS

PREVIOUS MAILING ADDRESS

(Fill in your previous mailing address ~f you have moved in the last 6 months.)

Note: not required by Equifax and Experian.

SOCIAL SECURITY NUMBER

Note: not required by Experian.

DATE OF BIRTH

Note: not required by Equifax and Experian.

Thank you for your prompt handling of my request.

SIGNATURE

Chart Your Course of Action

Use this form to record the steps you've taken to report the fraudulent use of your identity. Keep this list in a safe place for reference.

Credit Bureaus – Report Fraud

Bureau	Phone Number	Date Contacted	Contact Person	Comments
Equifax	1-800-525-6285			
Experian	1-888-397-3742			
Trans Union	1-800-680-7289			

Banks, Credit Card Issues and Other Creditors (Contact each creditor promptly to protect your legal rights.)

Creditor	Address and Phone Number	Date Contacted	Contact Person	Comments

Law Enforcement Authorities – Report Identity Theft

Agency/Dept	1-877-IDTHEFT	Date Contacted	Contact Person	Report Number	Comments
Federal Trade Commission					
Local Police Department					

