



Identity Theft

what you need
to know



CONTENTS

PAGE

What is identity theft?	3
How can someone steal my identity?	4
Fraudulent use of your personal information	5
Protecting yourself against identity theft	6
How can I tell if I'm a victim of identity theft?	7
Dealing with identity theft	8
Reclaiming your identity	14
Resolving identity theft-related credit problems	16
Sample dispute letter	20
Important information and contacts	23

At Citi, we want to keep you informed about all of the issues that can affect your financial life. We're bringing you helpful information provided to us by the Federal Trade Commission on how to protect yourself against identity theft and what to do if you become a victim. For more on credit card safety and fraud prevention tips, visit our website www.UseCreditWisely.com.

What is identity theft?

Identity theft happens when someone accesses essential elements of a person's identifying information in order to commit theft. This information includes name, address, Social Security number, date of birth and mother's maiden name. Many identity thieves use this personal information in order to open credit card accounts, obtain loans and even mortgages in the victim's name.

How can someone steal my identity?

Identity thieves may use a variety of methods to gain access to your personal information, such as:

- Stealing personal information from your home.
- Getting information from businesses or institutions by:
 - ▶ stealing records from their employer,
 - ▶ bribing an employee who has access to the records,
 - ▶ conning information out of employees, or
 - ▶ hacking into the organization's computers.
- Rummaging through your trash, the trash of businesses, or dumps in a practice known as "dumpster diving."
- Obtaining credit reports by abusing their employer's authorized access to credit reports or by posing as a landlord, employer or someone else who may have a legitimate need for and a legal right to the information.
- Stealing wallets and purses.
- Stealing mail, including bank and credit card statements, pre-approved credit offers, new checks, or tax information.
- Completing a "change of address form" to divert mail to another location.
- Obtaining information directly from you by posing as a legitimate businessperson or government official.

Fraudulent use of your personal information

Once thieves steal your personal information, they assume your identity to commit fraud, such as:

- Call your card issuer; ask to change the mailing address on your card account and request that a new card be sent to the new address. The imposter then runs up charges on your account.
- Open a new credit card account, using your name, date of birth and Social Security number.
- Establish phone or wireless service in your name.
- Open a bank account in your name to write bad checks.
- File for bankruptcy under your name to avoid paying debts they've incurred under your name or to avoid eviction.
- Buy cars by taking out auto loans in your name.
- Give your name to the police during an arrest.



Protecting yourself against identity theft

You can reduce your risk and safeguard your identifying information by following some simple guidelines.

- **Protect your mailbox:** Remove your mail as soon after delivery as possible. Also, deposit outgoing mail in post office collection boxes or at your local post office to lower the risk of identity theft happening to you.
- **Protect your wallet:** Keep items with personal information in a safe place at home and do not share this information with friends or acquaintances. Don't carry your Social Security card in your wallet or purse. Memorize your Social Security number and never write it down on anything you carry. Destroy all of your receipts when you no longer need them.
- **Protect your credit and debit cards:** Whenever you receive a new card, sign it immediately. Never loan your card to anyone, under any circumstance. Notify your bank and other issuers when you change your address or phone number and be sure to report all lost or stolen cards immediately. Never put your account number on the outside of any envelope.



How can I tell if I'm a victim of identity theft?

An identity thief can strike even if you've been very careful with your personal information. Some indications of identity theft may include:

- Failing to receive bills or other mail signaling an address change by the identity thief;
- Receiving cards or billing statements for accounts for which you did not apply;
- Receiving calls from debt collectors of companies about merchandise or services you didn't buy.

If you think you may be a victim, you can obtain a copy of your credit report from each of the three major credit bureaus listed on page 23. If it's accurate and includes only those activities you've authorized, chances are you're not a victim of identity theft.



Dealing with identity theft

If you suspect that your personal information has been stolen to commit fraud or theft, Citi can help. As a Citi card customer, you can automatically use the free services of Citi Identity Theft Solutions, even if the fraud occurred on a card from another issuer. At Citi, we constantly safeguard and protect your identity by monitoring your card account for any suspicious activity, often identifying fraud before you are aware – or the thief does damage. However, personal information can be stolen even without your card. Our team of Identity Theft Solutions specialists will provide personal support and assistance through the process of re-establishing your credit. They are available to you at 1-800-950-5114.

When you call to report fraudulent activities on your Citi card account or a card account that has been fraudulently opened in your name, we will begin an investigation immediately. Once it has been established that you are a victim of identity theft, a Specialist will be assigned to your case and work with you for the duration of the investigation. The Specialist will work with you to streamline and simplify the steps to reclaiming your identity, such as:

- Immediately close your existing unauthorized Citi card account to prevent further unauthorized charges and open a new card account for you.
- Assist you in contacting a credit bureau to check your credit report for fraudulent activity. The credit bureau will then place a “Fraud Alert” on your files at all three credit bureaus.
- Provide advice and information about contacting other creditors for your other card accounts or to close other unauthorized card accounts.
- Help you understand how to complete/submit a police report as well as other government-related forms that may be necessary for submission, depending upon the specifics of your case.
- Continue to monitor your credit bureau report and notify you quickly if any more fraud is detected until your case is closed.
- Continue to keep in touch with you about the status of your card account until the case is closed.

If you choose to handle this situation yourself, take action immediately, and keep a record of your conversations and correspondence. Exactly which steps you should take to protect yourself depends on your circumstances and how your identity has been misused. However, four basic actions are appropriate in almost every case.

Step 1: Contact the fraud departments of each of the three major credit bureaus.

• Equifax
1-800-525-6285

• Experian
1-888-397-3742

• TransUnion
1-800-680-7289

Tell them that you're an identity theft victim. Request that a "fraud alert" be placed in your file, as well as a "victim's statement" asking that the creditors call you before opening any new accounts or changing your existing accounts. This can help prevent an identity thief from opening additional accounts in your name.

At the same time, you will need to order copies of your credit report. If your requests are made in writing, credit bureaus are required to give you a free copy of your report if your report is inaccurate because of fraud (Contact information provided on page 23). Review your reports carefully to make sure no additional fraudulent accounts have been opened in your name or unauthorized charges have been made to your existing accounts. Check that information such as your Social Security number, address(es), name, and employers are correct. Also, check the section of your report that lists "inquiries." If "inquiries" appear from the company(ies) that opened the fraudulent account(s), request that these inquiries be removed from your report. In a few months, you should order new copies of your credit reports to verify that your corrections and changes have been made, and to make sure no new fraudulent activity has occurred.



Step 2: Close any accounts that have been tampered with or opened fraudulently.

Credit Accounts

Credit accounts include all accounts with banks, credit card companies and other lenders, and phone companies, utilities, Internet Service Providers (ISPs), and other service providers. Ask to speak with someone in the security or fraud department of each creditor and follow up with a letter. It's particularly important to notify credit card companies in writing because that's the consumer protection procedure the law spells out for resolving errors on credit card billing statements.

If there are fraudulent charges, ask the company about forms for disputing those transactions. Immediately close accounts that have been tampered with and open new ones with new Personal Identification Numbers (PINs) and passwords.

Checks

If your checks have been stolen or misused, close the account and ask your bank to notify the appropriate check verification service. While no federal law limits your losses if someone steals your checks and forges your signature, state laws may protect you.

You also should contact these major check verification companies directly for the following services:

• To request that they notify retailers who use their databases not to accept your checks, call:

Certegy, Inc.
1-800-437-5120

Global Payments
1-800-766-2748

TeleCheck
1-800-710-9898

• To find out if an identity thief has been passing bad checks in your name, call:

SCAN
1-800-262-7771

Step 3: File a police report with your local police or the police in the community where the identity theft took place.

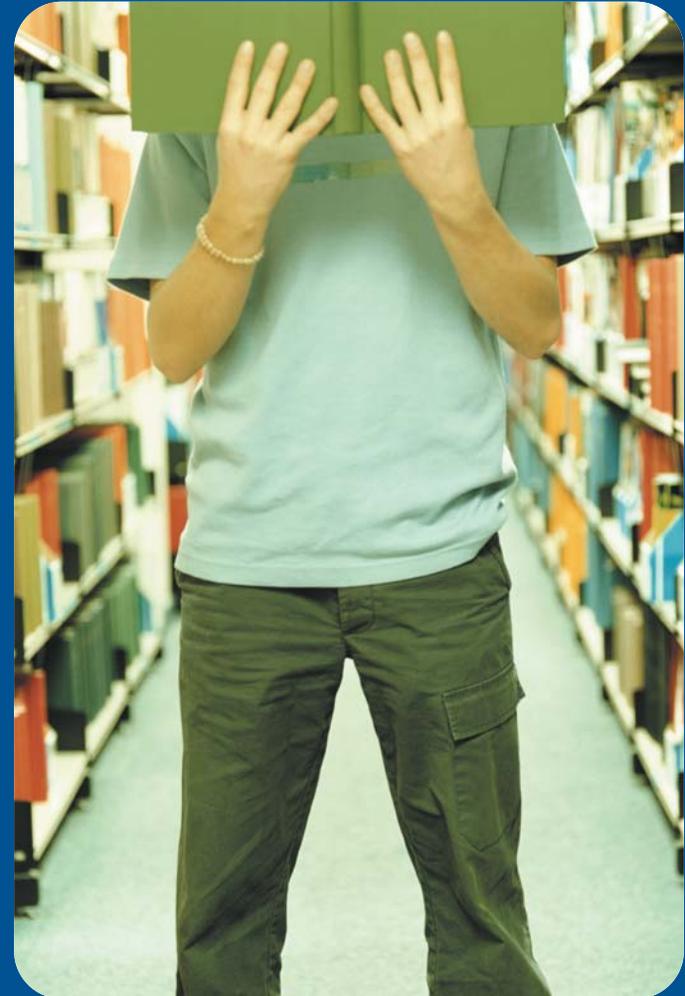
Even if the police can't catch the identity thief, having a copy of the police report can help you when dealing with creditors. Local authorities may tell you that they can't take a report. Stress the importance of a police report; many creditors require one to resolve your dispute. If you can't get the local police to take a report, try your county sheriff. If that doesn't work, try your state police or state law enforcement authorities. If you're told that identity theft is not a crime under your state law, ask to file a Miscellaneous Incident Report instead.

Get a copy of the police report in case the bank, credit card company or others need proof of the crime. If you can't get a copy, at least get the report number.

Step 4: File a complaint with the Federal Trade Commission (FTC)

Contact the FTC's Identity Theft Hotline by telephone: 1-877-IDTHEFT (438-4338); TDD: 202-326-2502; online at www.consumer.gov/idtheft; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The FTC enters complaints into a secure consumer fraud database, accessible only to law enforcement agencies, for use in pursuing criminal investigations.

“Once thieves steal your personal information, they assume your identity to commit fraud.”



Reclaiming your identity

The following steps can help you straighten out the damage done by identity theft.

Stolen Mail: If an identity thief has stolen your mail to get new credit cards, bank and credit card statements, pre-screened credit offers or tax information, or if an identity thief has falsified change-of-address forms, that's a crime. Report it to your local postal inspector.

Change of Address on credit or debit card accounts: If you discover that an identity thief has changed the billing address on an existing 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.

Bank Accounts: If you have reason to believe that an identity thief has tampered with your bank accounts, checks or ATM card, close the accounts immediately. When you open new accounts, insist on password-only access to minimize the chance that an identity thief can violate the accounts. If your ATM card has been lost, stolen or otherwise compromised, cancel the card as soon as you can and get another with a new PIN.

Investments: If you believe that an identity thief has tampered with your securities investments or brokerage account, immediately report it to your broker or account manager and to the Securities and Exchange Commission, 202-942-8088.



Phone or wireless service: If an identity thief has established new phone or wireless service in your name; 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/or calling card. Open new accounts and choose new PINs.

Employment: If someone is using your Social Security number to apply for a job or to work, that's a crime. Report it to the Social Security Administration's Fraud Hotline at 1-800-269-0271.

Driver's license: If you suspect that your name or Social Security number is being used by an identity thief to get a driver's license or a non-driver's ID card, report it to your Department of Motor Vehicles. If your state uses your Social Security number as your driver's license number, ask to substitute another number.

Bankruptcy: If you believe someone has filed for bankruptcy using your name, write to the U.S. Trustee in the region where the bankruptcy was filed. A listing of the U.S. Trustee Program's regions can be found at www.usdoj.gov/ust or look in the Blue Pages of your phone book under U.S. Government-Bankruptcy Administration.

Criminal records/arrests: In rare instances, an identity thief may create a criminal record in your name. For example, your imposter may give your name when arrested. If this happens to you, you may need to hire an attorney to help resolve the problem. Contact a lawyer in your state or area (you may want to contact your local bar association for help in finding an attorney).

Resolving identity theft-related credit problems

Resolving credit problems resulting from identity theft can be time-consuming and frustrating. The good news is that there are federal laws that establish procedures for correcting credit report errors and billing errors, and for stopping debt collectors from contacting you about debts you don't owe.

The Fair Credit Reporting Act (FCRA) establishes procedures for correcting mistakes on your credit record. Under the FCRA, both the credit bureau and the organization that provided the information to the credit bureau (the "information provider"), such as a bank or credit card company, are responsible for correcting inaccurate or incomplete information in your report.



Dealing with credit bureaus

To protect your rights under the law, contact both the credit bureau and the information provider. First, call the credit bureau and then follow up in writing. Tell them what information you believe is inaccurate. Include copies (NOT originals) of documents that support your position. In addition to providing your complete name and address, your letter should clearly identify each item in your report that you dispute, give the facts and explain why you dispute the information, and request deletion or correction. You may want to enclose a copy of your credit bureau report with circles around the items in question.

Send your letter by certified mail, and request a return receipt so you can document what the credit bureau received and when. Keep copies of your dispute letter and enclosures.

Credit bureaus must usually investigate the items in question within 30 days. They also must forward all relevant data you provide about the dispute to the information provider. After the information provider receives notice of a dispute from the credit bureau, it must investigate, review all relevant information provided by the credit bureau, and report the results to the credit bureau.

If the information provider finds the disputed information to be inaccurate, it must notify any nationwide credit bureau that it reports to so that the credit bureau can correct this information in your file. Note that:

- Disputed information that cannot be verified must be deleted from your file.
- If your report contains erroneous information, the credit bureau must correct it.



- If an item is incomplete, the credit bureau must complete it.
- If your file shows an account that belongs to someone else, the credit bureau must delete it.

When the investigation is complete, the credit bureau must give you written results and a free copy of your report if the dispute results in a change. If an item is changed or removed, the credit bureau cannot put the disputed information back in your file unless the information provider verifies its accuracy and completeness, and the credit bureau gives you a written notice that includes the name, address and phone number of the information provider.

If you request a correction, the credit bureau must send notices of the corrections to anyone who received your report in the past six months. Job applicants can have a corrected copy of their report sent to anyone who received a copy during the past two years for employment purposes. If an investigation does not resolve your dispute, ask the credit bureau to include your statement of the dispute in your file and in future reports.

Dealing with creditors/information providers

In addition to writing to the credit bureau, tell the creditor or other information providers in writing that you dispute an item (see sample dispute letter below). Again, include copies (NOT originals) of documents that support your position. If the information provider then reports the item to any credit bureau, it must include a notice of your dispute. In addition, if you are correct - that is, if the disputed information is not accurate - the information provider must not use it again.

Sample Dispute Letter

This is a sample letter that you can use to dispute false or inaccurate information on your credit report. Areas highlighted in *italics* should be changed to fit your personal situation.

Date
Your Name
Your Address
Your City, State, Zip Code

Complaint Department
Name of Credit Bureau
Address
City, State, Zip Code

Dear Sir or Madam:

I am writing to dispute the following information in my file. The items I dispute also are circled on the attached copy of the report I received. *(Identify item(s) disputed by name of source, such as creditors or tax court, and identify type of item, such as credit account, judgment, etc.)*

This item is *(inaccurate or incomplete)* because *(describe what is inaccurate or incomplete and why)*. I am requesting that the item be deleted *(or request another specific change)* to correct the information.

Enclosed are copies of *(use this sentence if applicable and describe any enclosed documentation, such as payment records, court documents)* supporting my position. Please investigate this *(these)* matter(s) and *(delete or correct)* the disputed item(s) as soon as possible. Please confirm to me in writing when this has been completed.

Sincerely,
(Your name)
Enclosures: *(List what you are enclosing.)*



Important information and contacts



Citi Credit Cards

For assistance, call the number on the back of your card, or call 1-800-950-5114.

CitiPhone Banking®

For assistance, call the number on the back of your card, or call 1-800-274-6660.

Stolen Checks or Fraudulent Bank Accounts

If your checks are stolen or you believe your bank account has been compromised, you should call each of the following companies:

Certegy, Inc.
1-800-437-5120

Global Payments
1-800-766-2748

TeleCheck
1-800-710-9898

SCAN
1-800-262-7771

Federal Trade Commission (FTC)

Identity Theft Clearing House
600 Pennsylvania Avenue NW
Washington, DC 20580
www.consumer.gov/idtheft
1-877-IDTHEFT

Social Security Administration's Fraud Hotline

P.O. Box 17768
Baltimore, MD 21235
www.ssa.gov/oig
1-800-269-0271

U.S. Postal Inspector

www.usps.gov/websites/depart/inspect
See your local telephone directory

Credit Bureaus

Equifax

To report fraud, call 1-800-525-6285, and write:
P.O. Box 740241
Atlanta, GA 30374-0241
www.econsumer.equifax.com
For a credit report call 1-800-685-1111

Experian

To report fraud, call 1-888-397-3742, and write:
P.O. Box 9532
Allen TX, 75013
www.experian.com/consumer
For a credit report call 1-888-397-3742

TransUnion

To report fraud, call 1-800-680-7289, and write:
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com
For a credit report call 1-800-916-8800

