

# Identity Theft

---

## A Recovery Plan



FEDERAL TRADE COMMISSION

[IdentityTheft.gov](http://IdentityTheft.gov)

**Visit [IdentityTheft.gov](http://IdentityTheft.gov) for our most up-to-date information.**

---

The site provides detailed advice to help you fix problems caused by identity theft, along with the ability to:

- get a **personal recovery plan** that walks you through each step
- **update** your plan and **track** your progress
- print **pre-filled letters & forms** to send to credit bureaus, businesses, and debt collectors
- **report** it to the Federal Trade Commission

Go to **[IdentityTheft.gov](http://IdentityTheft.gov)** and click "**Get Started.**"

# About Identity Theft

If someone is using your personal or financial information to make purchases, get benefits, file taxes, or commit fraud, that's identity theft. This booklet can guide you through the recovery process.

If you're dealing with tax, medical, or child identity theft, read **Special Forms of Identity Theft** (page 13).

If you've had personal or financial information lost or stolen, see **Data Breaches and Lost or Stolen Info** (page 28).

## Table of Contents

What To Do Right Away	1
What To Do Next	3
Other Possible Steps	6
Steps for Certain Accounts	9
Special Forms of Identity Theft	13
Sample Letters and Memo	17
Know Your Rights	25
Data Breaches and Lost or Stolen Info	28
Annual Credit Report Request Form	31





# What To Do Right Away

## Step 1: Call the companies where you know fraud occurred.

- ☐ Call the fraud department. Explain that someone stole your identity.
- ☐ Ask them to close or freeze the accounts. Then, no one can add new charges unless you agree.
- ☐ Change logins, passwords, and PINs for your accounts.

You might have to contact these companies again after you have an Identity Theft Report.

## Step 2: Place a fraud alert and get your credit reports.

- ☐ To place a free fraud alert, contact one of the three credit bureaus. That company must tell the other two.
  - **Experian.com/help**  
888-EXPERIAN (888-397-3742)
  - **TransUnion.com/credit-help**  
888-909-8872
  - **Equifax.com/personal/credit-report-services**  
800-685-1111

Get updates at **IdentityTheft.gov/creditbureaucontacts**.

A fraud alert lasts one year. It will make it harder for someone to open new accounts in your name.

You'll get a letter from each credit bureau. It will confirm that they placed a fraud alert on your file.

- ☐ Get your free credit reports from Equifax, Experian, and TransUnion. Go to **annualcreditreport.com** or call 1-877-322-8228.

Did you already order your free annual reports this year? If so, you can pay to get your report immediately. Or follow the instructions in the fraud alert confirmation letter from each credit bureau to get a free report. That might take longer.

- ☐ Review your reports. Make note of any account or transaction you don't recognize. This will help you report the theft to the Federal Trade Commission (FTC) and the police.

### Step 3: Report identity theft to the FTC.

- Go to **IdentityTheft.gov** or call 1-877-438-4338. Include as many details as possible.

Based on the information you enter, **IdentityTheft.gov** will create your Identity Theft Report and recovery plan.

- If you create an account, we'll walk you through each recovery step, update your plan as needed, track your progress, and pre-fill forms and letters for you.
- If you don't create an account, you must print and save your Identity Theft Report and recovery plan right away. Once you leave the page, you won't be able to access or update them.

Your Identity Theft Report is important because it guarantees you certain rights. You can learn more about your rights on page 25.

# What To Do Next

Take a deep breath and begin to repair the damage.

## Close new accounts opened in your name.

- ☐ Now that you have an Identity Theft Report, call the fraud department of each business where an account was opened.
  - Explain that someone stole your identity.
  - Ask the business to close the account.
  - Ask the business to send you a letter confirming that:
    - the fraudulent account isn't yours
    - you aren't liable for it
    - it was removed from your credit report
  - Keep this letter. Use it if the account appears on your credit report later on.

The business may require you to send them a copy of your Identity Theft Report or complete a special dispute form. The sample letter on page 18 can help.

- ☐ Write down who you contacted and when.

## Remove bogus charges from your accounts.

- ☐ Call the fraud department of each business.
  - Explain that someone stole your identity.
  - Tell them which charges are fraudulent. Ask the business to remove the charges.
  - Ask the business to send you a letter confirming they removed the fraudulent charges.
  - Keep this letter. Use it if these charges appear on your credit report later on.

The business may require you to send them a copy of your Identity Theft Report or complete a special dispute form. The sample letter on page 19 can help.

- ☐ Write down who you contacted and when.

## Correct your credit report.

- Write to each of the three credit bureaus. The sample letter on page 20 can help.
  - Include a copy of your Identity Theft Report and proof of your identity, like a copy of your driver's license or state ID.
  - Explain which information on your report is fraudulent.
  - Ask them to block that information. Mail your letters to:
    - **TransUnion**  
Fraud Victim Assistance Department  
P.O. Box 2000  
Chester, PA 19022-2000
    - **Equifax**  
P.O. Box 105069  
Atlanta, GA 30348-5069
    - **Experian**  
P.O. Box 9554  
Allen, TX 75013

If someone steals your identity, you have the right to remove fraudulent information from your credit report. This is called blocking. Once the information is blocked, it won't show up on your credit report, and companies can't try to collect the debt from you. If you have an Identity Theft Report, credit bureaus must honor your request to block fraudulent information. Use the sample letter on page 20 to block information.

If you don't have an Identity Theft Report, you still can dispute incorrect information in your credit file. It can take longer, and there's no guarantee that the credit bureaus will remove the information. To dispute information without an Identity Theft Report, contact each credit bureau online or by phone.



## Consider adding an extended fraud alert or credit freeze.

Extended fraud alerts and credit freezes can help prevent further misuse of your personal information. There are important differences. This chart can help you decide which might be right for you.

<b>An Extended Fraud Alert</b>	<b>A Credit Freeze</b>
Lets you have access to your credit report as long as companies take steps to verify your identity	Restricts access to your credit report unless you lift or remove the freeze
Free to place and remove. Available if someone stole your identity.	Free to place and remove. Available to anyone.
Lasts for seven years	Lasts until you lift or remove
Set it by contacting one credit bureau. That one must notify the other two. <ul style="list-style-type: none"><li>• Report that someone stole your identity</li><li>• Request an extended fraud alert</li><li>• Complete any necessary forms and send a copy of your Identity Theft Report</li></ul>	Set it by contacting each of the three credit bureaus.
<p><b>Experian.com/help</b> 888-EXPERIAN (888-397-3742)</p> <p><b>TransUnion.com/credit-help</b> 888-909-8872</p> <p><b>Equifax.com/personal/credit-report-services</b> 800-685-1111</p> <p>Get updates at <b>IdentityTheft.gov/creditbureaucontacts</b>.</p>	

# Other Possible Steps

Depending on your situation, you might need to take additional steps.

## Report a misused Social Security number.

- ☐ Do you think someone else is using your Social Security number for work? Review your Social Security work history by creating an account at **ssa.gov/myaccount**. If you find errors, contact your local Social Security Administration (SSA) office.

## Stop debt collectors from trying to collect debts you don't owe.

- ☐ Write to the debt collector within 30 days of getting the collection letter. The sample letter on page 21 can help.
  - Tell the debt collector someone stole your identity, and you don't owe the debt.
  - Send copies of your Identity Theft Report and any other documents that detail the theft.
- ☐ Contact the business where the fraudulent account was opened.
  - Explain that this is not your debt.
  - Tell them to stop reporting this debt to the credit bureaus.
  - Ask for information about the debt, and how it happened. The business must give you details if you ask.

For example, if someone opened a credit card in your name, ask for a copy of the application and the applicant's signature.

- ☐ If you haven't already, ask the credit bureaus to block information about this debt from your credit report.

The advice in **What To Do Next** on page 4 can help you block fraudulent information from your credit reports.

- ☐ Write down who you contacted and when. Keep copies of any letters you send or receive.



## File a report with your local police department.

Your Identity Theft Report (from **IdentityTheft.gov**) is an official report to law enforcement. This report is sufficient documentation to resolve issues with the credit bureaus and most companies. However, you'll want to report to local police if you have information about a suspect — or a specific company asks for a police report as part of its dispute resolution process.

- ☐ Go to your local police office with:
  - a copy of your FTC Identity Theft Report
  - a government-issued ID with a photo
  - proof of your address (mortgage statement, rental agreement, or utilities bill)
  - any other proof you have of the theft — bills, Internal Revenue Service (IRS) notices, etc.
- ☐ Tell the police someone stole your identity and you need to file a report.
- ☐ Ask for a copy of the police report.

## Replace government-issued IDs.

- ☐ Social Security card lost or stolen? Apply online at **ssa.gov/ssnumber** to get a free replacement card.
- ☐ Driver's license lost or stolen? You can find your nearest motor vehicles office at **usa.gov/Motor-Vehicle-Services**.

The state might flag your license number in case someone else tries to use it, or they might suggest that you apply for a replacement license.

- ☐ Passport lost or stolen? Call the State Department at 1-877-487-2778 or TTY 1-888-874-7793. If you want to replace the passport, you have several options:
  - If you **are** traveling within the next two weeks, make an appointment to apply in person at a Passport Agency or Center.
  - If you **are not** traveling within two weeks, submit Form DS-11 and DS-64 in person at an authorized Passport Application Acceptance Facility.

## Clear your name of criminal charges.

- If someone is arrested and uses your name or personal information, contact the law enforcement agency that arrested the thief. You may need to check court records to find out where the thief was arrested.
    - File a report about the impersonation.
    - Give copies of your fingerprints, photograph, and identifying documents.
    - Ask the law enforcement agency to:
      - compare your information to the imposter's
      - change all records from your name to the imposter's name (if you know it)
      - give you a "clearance letter" or "certificate of release" to declare your innocence
    - Keep the "clearance letter" or "certificate of release" with you at all times.
    - Write down who you contacted and when.
  - If a court prosecutes an identity thief using your name, contact the court where the arrest or conviction happened.
    - Ask the district attorney for records to help you clear your name in court records.
    - Provide proof of your identity.
    - Ask the court for a "certificate of clearance" that declares you are innocent.
    - Keep the "certificate of clearance" with you at all times.
  - Contact your state Attorney General. You can find contact information at [usa.gov/state-consumer](https://www.usa.gov/state-consumer).
    - Ask if your state has an "identity theft passport" — a tool you can use to resolve financial issues related to the identity theft — or some other special help for identity theft victims.
      - If you get an identity theft passport, keep it with you at all times.
  - Consider hiring a criminal defense lawyer. Your state or local bar association can help you find a lawyer.
  - Ask the law enforcement agency that arrested the thief which information brokers buy their records.
    - Write to the brokers. Ask them to remove errors from your file.
- Information brokers buy criminal records and sell information to employers and debt collectors.
- Write down who you contacted and when. Keep copies of any letters you send or receive.

# Steps for Certain Accounts

For certain types of accounts, you might have to contact additional offices.

- Utilities
- Phones
- Government Benefits
- Checking Accounts
- Student Loans
- Apartment or House Rentals
- Investment Accounts
- Bankruptcy

## Utilities

- ☐ If someone used your information to get cable, electric, water, or other similar services, contact the service provider.
  - Tell them someone stole your identity and ask them to close the account.
- ☐ For additional help, contact your state Public Utility Commission and explain the situation. You can find contact information at [naruc.org/about-naruc/regulatory-commissions](http://naruc.org/about-naruc/regulatory-commissions).
- ☐ Write down who you contacted and when. Keep copies of any letters you send or receive.

## Phones

- ☐ Contact the National Consumer Telecom and Utilities Exchange and request your NCTUE® Data Report. Review it for any accounts you don't recognize.
  - **nctue.com**  
1-866-349-5185

What is the NCTUE Data Report? The NCTUE Data Report is a record of all telecommunication, pay TV, and utility accounts reported by exchange members, including information about your account history, unpaid accounts, and customer service applications.

- ☐ If the service provider doesn't resolve the problem, file a complaint with the Federal Communications Commission at [consumercomplaints.fcc.gov](http://consumercomplaints.fcc.gov) or 1-888-225-5322 or TTY 1-888-835-5322.



## Government Benefits

- ☐ Contact the agency that issued the government benefit and explain that someone stole your identity. You can find local government agencies at [usa.gov/local-governments](https://www.usa.gov/local-governments).

For Social Security benefits, contact the SSA Office of the Inspector General at [oig.ssa.gov](https://oig.ssa.gov) or 1-800-269-0271.

- ☐ Ask what you need to do to fix the problem.
- ☐ If you stopped receiving your benefits because of the identity theft, ask what you need to do to get them reinstated. You may need to appear in person or send something in writing.
- ☐ Make a note of who you contacted and when.

## Checking Accounts

- ☐ Do you think someone opened a checking account in your name? Order a free copy of your ChexSystems report, which compiles information about your checking accounts.
  - To get your report, contact ChexSystems at 1-800-428-9623.
  - Then contact every financial institution where a new account was opened. Ask them to close the accounts.
- ☐ If someone is writing bad checks against your account, contact your financial institution.
  - Ask them to stop payment on stolen checks and close your account.
  - Ask them to report the theft to their check verification system. The check verification system will tell businesses to refuse the stolen checks.
  - Contact any business that took the bad check. Explain that someone stole your identity. Act quickly, before they start collection action against you.

You also can contact check verification companies. Report that your checks were stolen. Ask them to tell businesses to refuse the stolen checks.

- Telecheck: 1-800-710-9898
- Certegy: 1-800-437-5120

- ☐ If a business rejects your check, ask the business for an explanation. The business must tell you what information led them to reject your check.
- ☐ Write down who you contacted and when. Keep copies of any letters you send or receive.

## Student Loans

- ☐ Contact the school or program that opened the loan.
  - Explain the situation.
  - Ask them to close the loan, and send you a letter that says you aren't responsible for the loan.

- ☐ If this is a federal student loan, contact the U.S. Department of Education Office of Inspector General hotline at 1-800-MISUSED (1-800-647-8733).

If these steps don't resolve your situation, contact the U.S. Department of Education Federal Student Aid Ombudsman at 1-877-557-2575.

- ☐ Write down who you contacted and when. Keep copies of any letters you send or receive.

## Apartment or House Rentals

- ☐ Ask the landlord who rented the property to the identity thief what tenant history services they use. Contact those companies. Ask for a copy of your tenant history report, and ask what steps you need to take to correct fraudulent information in the report.

What's a tenant history report? There are several companies that collect and sell information about renters – such as how often a renter was late or if a renter has ever been evicted. If someone leased an apartment in your name, you'll want to correct any errors in your tenant history reports.

- ☐ Write down who you contacted and when. Keep copies of any letters you send or receive.

## Investment Accounts

- ☐ Call your broker or account manager, and describe the situation.
- ☐ Write down who you contacted and when. Keep copies of any letters you send or receive.

## Bankruptcy

- ☐ Visit **usdoj.gov/ust** to find the U.S. Trustee in the region where the bankruptcy was filed. Write to the office and describe the situation. Provide proof of your identity.

The U.S. Trustee Program refers cases of suspected bankruptcy fraud to the U.S. Attorneys for possible prosecution. The U.S. Trustee can't give you legal help, so you may need to hire an attorney.

- 
- ☐ Consider hiring an attorney. Your state or local bar association can help you find a lawyer.

An attorney can explain to the court that the bankruptcy filing was fraudulent.

- 
- ☐ Write down who you contacted and when. Keep copies of any letters you send or receive.



# Special Forms of Identity Theft

- Tax Identity Theft
- Child Identity Theft
- Medical Identity Theft

## Tax Identity Theft

- ☐ If you get an IRS notice in the mail that says someone used your Social Security number to get a tax refund, follow the instructions provided in the letter.

Complete IRS Form 14039, Identity Theft Affidavit. Mail or fax the form according to the instructions. Or you can complete and submit IRS Form 14039 online, using **IdentityTheft.gov**.

- ☐ Did the notice say you were paid by an employer you don't know? Send a letter to the employer explaining that someone stole your identity, and that you don't work for the employer.

- ☐ File your tax return, and pay any taxes you owe.

You might have to mail paper tax returns.

- ☐ Write down who you contacted and when. Keep copies of any letters you send or receive.

If these steps don't resolve your situation, contact the IRS for specialized assistance at 1-800-908-4490.

- ☐ Place a fraud alert. Contact one of the three credit bureaus. That company must tell the other two.

- **Experian.com/help**  
888-EXPERIAN (888-397-3742)
- **TransUnion.com/credit-help**  
888-909-8872
- **Equifax.com/personal/credit-report-services**  
800-685-1111

Get updates at **IdentityTheft.gov/creditbureaucontacts**.

- ☐ Get your free credit reports from TransUnion, Experian, and Equifax. Go to **annualcreditreport.com** or call 1-877-322-8228.

Review your reports. If you find any accounts or charges you don't recognize, go to **IdentityTheft.gov** to report the theft and follow the steps in your recovery plan.

## Child Identity Theft

- Did someone use your child's information to commit fraud? Call the company where the fraud occurred.
  - Explain that someone stole your child's identity and opened a fraudulent account. Explain that your child is a minor, and cannot enter into legal contracts.
  - Ask them to close the fraudulent account and send you a letter confirming that your child isn't liable for the account.
  - Send a follow-up letter and include a copy of your child's birth certificate.
  - Make a note of who you contacted and when.

Did someone file taxes using your child's Social Security number? Complete IRS Form 14039, Identity Theft Affidavit. Mail or fax the form according to the instructions. Or complete and submit IRS Form 14039 online, using **IdentityTheft.gov**. If that doesn't resolve the problem, contact the IRS for specialized assistance at 1-800-908-4490.

- To find out if your child has a credit report, request a manual search for your child's Social Security number. Each credit bureau has its own process for this:
  - <https://www.Experian.com/fraudalert> – Click on “Minor Child Instructions” under “Additional Resources”
  - <https://www.Transunion.com/credit-disputes/child-identity-theft-inquiry-form.page>
  - <https://help.equifax.com/s/article/How-do-I-get-a-copy-of-my-childs-credit-reports>

Why check for a credit report? Generally, children won't have credit reports – unless someone is using their information for fraud.

- If a credit bureau has a credit report for your child, they will send you a copy of the report. To remove fraudulent accounts, follow the instructions provided with the credit report.
- Request a freeze to make it more difficult for someone to use your child's Social Security number to open accounts. To place a freeze, follow the specific instructions for each credit bureau at:
  - **Experian.com/help**  
888-EXPERIAN (888-397-3742)
  - **TransUnion.com/credit-help**  
888-909-8872
  - **Equifax.com/personal/credit-report-services**  
800-685-1111

Get updates at **IdentityTheft.gov/creditbureaucontacts**.

## Medical Identity Theft

- ☐ If you suspect that someone used your information to get medical services, get copies of your medical records:
  - Contact each doctor, clinic, hospital, pharmacy, laboratory, and health plan where the thief may have used your information. Ask for copies of your medical records.
  - Complete the providers' records request forms and pay any fees required to get copies of your records.
  - Check your state's health privacy laws. Some state laws make it easier to get copies of your medical records.

Federal law gives you the right to know what's in your medical files.

Did your provider refuse to give you copies of the records to protect the identity thief's privacy rights? You can appeal. Contact the person listed in your provider's Notice of Privacy Practices, the patient representative, or the ombudsman. Explain the situation and ask for your file.

If the provider refuses to provide your records within 30 days of your written request, you may complain to the U.S. Department of Health and Human Services Office for Civil Rights at [hhs.gov/ocr](https://www.hhs.gov/ocr).

- ☐ Review your medical records. If you find any fraudulent information, go to **IdentityTheft.gov** and report it. This will create an official Identity Theft Report.
- ☐ Report any errors to your health care provider.
  - Write to your health care provider to report mistakes in your medical records.
  - Include a copy of the medical record showing the mistake.
  - Explain why this is a mistake, and how to correct it.
  - Include a copy of your Identity Theft Report.
  - Send the letter by certified mail, and ask for a return receipt.

Your health care provider should respond to your letter within 30 days. Ask the provider to fix the mistake and notify other health care providers who may have the same mistake in their records.

- ☐ Notify your health insurer.
  - Send your Identity Theft Report to your health insurer's fraud department. Tell them about any errors in your medical records.
- ☐ If there are medical billing errors on your credit report, notify all three credit bureaus by following the steps under **What to Do Next** on page 3.
- ☐ Write down who you contacted and when. Keep copies of any letters you send or receive.





# Sample Letters and Memo

If you create a free account at **IdentityTheft.gov**, you can get these letters pre-filled with your information.

## Letters

- Identity Theft Letter About a Fraudulent Account
- Identity Theft Letter About Fraudulent Charges to Your Account
- Identity Theft Letter to a Credit Bureau
- Identity Theft Letter to a Debt Collector

Additional letters are available at **IdentityTheft.gov/sample-letters**.

## Memo

- Notice to Furnishers of Information

# Identity Theft Letter About a Fraudulent Account

This sample letter will help you dispute and close a fraudulent account that was opened by an identity thief.

The text in [brackets] indicates where you must customize the letter.

---

[Date]

[Your Name]

[Your Address]

[Your City, State, Zip Code]

[Name of Company]

[Fraud Department]

[Address]

[City, State, Zip Code]

[RE: Your Account Number (if known)]

Dear Sir or Madam:

I am a victim of identity theft. I recently learned that my personal information was used to open an account at your company. I did not open or authorize this account, and I request that it be closed immediately. Please send me written confirmation that I am not responsible for charges on this account, and take appropriate steps to remove information about this account from my credit files.

I have enclosed a copy of my Identity Theft Report and proof of my identity. I also have enclosed a copy of the Notice to Furnishers of Information, which explains your responsibilities when reporting information to credit bureaus. When you receive a request like this with an Identity Theft Report, you must stop reporting fraudulent debts to credit bureaus.

The Notice also states that if a credit bureau notifies you that information you provided may be the result of identity theft, you must stop reporting the inaccurate information and you cannot attempt to sell or transfer the fraudulent debts to another party for collection.

Please send me a letter explaining your findings and actions.

Sincerely,

[Your Name]

Enclosures: [List what you are enclosing]

- Identity Theft Report
- Proof of Identity [a copy of your driver's license or state ID]
- Notice to Furnishers of Information [pp. 23-24]



# Identity Theft Letter About Fraudulent Charges to Your Account

This sample letter will help you dispute fraudulent charges on your accounts.

The text in [brackets] indicates where you must customize the letter.

---

[Date]

[Your Name]

[Your Address]

[Your City, State, Zip Code]

[Name of Company]

[Fraud Department]

[Address]

[City, State, Zip Code]

[RE: Your Account Number (if known)]

Dear Sir or Madam:

I am a victim of identity theft, and I am writing to dispute the following fraudulent charges on my account:

- [list charges, amounts, and dates of fraudulent transactions]

I did not make the charges listed above. I request that you remove all fraudulent charges and any related fees, send me an updated and accurate statement, and close the account. I also request that you stop reporting the inaccurate information to credit bureaus.

I have enclosed my Identity Theft Report and proof of my identity. I also have enclosed a copy of the Notice to Furnishers of Information, which explains your responsibilities when providing information to credit bureaus.

The Notice also states that if a credit bureau notifies you that information you provided may be the result of identity theft, you must stop reporting the inaccurate information and you cannot attempt to sell or transfer the fraudulent debts to another party for collection.

Please investigate this matter and send me a written explanation of your findings and actions.

Sincerely,

[Your Name]

Enclosures: [List what you are enclosing]

- Identity Theft Report
- Proof of Identity [a copy of your driver's license or state ID]
- Notice to Furnishers of Information [pp. 23-24]

# Identity Theft Letter to a Credit Bureau

This sample letter will help remove inaccurate information on your credit report.

The text in [brackets] indicates where you must customize the letter.

---

[Date]

[Your Name]

[Your Address]

[Your City, State, Zip Code]

(Write to each relevant credit bureau, one at a time:)

Equifax

P.O. Box 105069

Atlanta, GA 30348-5069

or

Experian

P.O. Box 9554

Allen, TX 75013

or

TransUnion

Fraud Victim Assistance Department

P.O. Box 2000

Chester, PA 19022-2000

[RE: Your Account Number (if known)]

Dear Sir or Madam:

I am a victim of identity theft. The information listed below, which appears on my credit report, does not relate to any transaction(s) that I have made. It is the result of identity theft.

[Identify item(s) resulting from the identity theft that should be blocked, by name of the source, such as the credit card issuer or bank, and type of item, such as credit account, checking account, etc.]

I have enclosed my Identity Theft Report, proof of my identity, and a copy of my credit report showing fraudulent items.

Please block this information from my credit report, pursuant to section 605B of the Fair Credit Reporting Act, and send the required notifications to all furnishers of this information.

I appreciate your prompt attention to this matter, and await your reply.

Sincerely,

[Your Name]

Enclosures: [List what you are enclosing]

- Identity Theft Report
- Proof of Identity [a copy of your driver's license or state ID]
- Copy of Credit Report

# Identity Theft Letter to a Debt Collector

This sample letter will help you request that a debt collector stop collecting debts that you don't owe.

The text in [brackets] indicates where you must customize the letter.

---

[Date]

[Your Name]

[Your Address]

[Your City, State, Zip Code]

[Name of Credit Collection Company]

[Company Address]

[City, State, Zip Code]

[RE: Your Account Number (if known)]

I am a victim of identity theft. An identity thief used my personal information without my permission to make purchases with [name of business where account was opened]. This debt is not mine. I have enclosed proof of my identity and a copy of my Identity Theft Report.

In accordance with the Fair Debt Collection Practices Act, I am asking you to immediately stop all collection activities about this debt, and stop reporting it to credit bureaus. I also ask that you tell the business where the account was opened that this debt is the result of identity theft.

I have enclosed a copy of the Notice to Furnishers of Information. It explains your responsibilities under the Fair Credit Reporting Act (FCRA). The FCRA requires that debt collectors give an identity theft victim documents related to an account if the victim asks. Please send me copies of all records relating to the account, including:

- Account applications made on paper, online, or by telephone
- Account statements or invoices
- Records of payment or charge slips
- Delivery addresses associated with the account
- Records of phone numbers used to activate or access the account
- Signatures on applications and accounts
- Investigator's report

Please send me a letter explaining what you have done to:

- Inform the business where the account was opened that the debt is the result of identity theft
- Stop collection activities against me
- Stop reporting information about the debt to credit bureaus
- If you've already reported the debt to credit bureaus, notify them that the debt is the result of identity theft
- Provide me with the records I request

(continued on next page)

Thank you for your cooperation.

Sincerely,

[Your Name]

Enclosures: [List what you are enclosing]

- Proof of Identity [a copy of your driver's license or state ID]
- Identity Theft Report
- Notice to Furnishers of Information [pp. 23-24]



All furnishers of information to consumer reporting agencies must comply with all applicable regulations. Information about applicable regulations currently in effect can be found at the Consumer Financial Protection Bureau's website, [consumerfinance.gov/learnmore](http://consumerfinance.gov/learnmore).

## NOTICE TO FURNISHERS OF INFORMATION: OBLIGATIONS OF FURNISHERS UNDER THE FCRA

The federal Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681-1681y, imposes responsibilities on all persons who furnish information to consumer reporting agencies (CRAs). These responsibilities are found in Section 623 of the FCRA, 15 U.S.C. § 1681s-2. State law may impose additional requirements on furnishers. All furnishers of information to CRAs should become familiar with the applicable laws and may want to consult with their counsel to ensure that they are in compliance. The text of the FCRA is available at the website of the Consumer Financial Protection Bureau (CFPB): [consumerfinance.gov/learnmore](http://consumerfinance.gov/learnmore). A list of the sections of the FCRA cross-referenced to the U.S. Code is at the end of this document.

Section 623 imposes the following duties upon furnishers:

### **Accuracy Guidelines**

The FCRA requires furnishers to comply with federal guidelines and regulations dealing with the accuracy of information provided to CRAs by furnishers. Federal regulations and guidelines are available at [consumerfinance.gov/learnmore](http://consumerfinance.gov/learnmore). Section 623(e).

### **General Prohibition on Reporting Inaccurate Information**

The FCRA prohibits information furnishers from providing information to a CRA that they know or have reasonable cause to believe is inaccurate. However, the furnisher is not subject to this general prohibition if it clearly and conspicuously specifies an address to which consumers may write to notify the furnisher that certain information is inaccurate. Sections 623(a)(1)(A) and (a)(1)(C).

### **Duty to Correct and Update Information**

If at any time a person who regularly and in the ordinary course of business furnishes information to one or more CRAs determines that the information provided is not complete or accurate, the furnisher must promptly provide complete and accurate information to the CRA. In addition, the furnisher must notify all CRAs that received the information of any corrections, and must thereafter report only the complete and accurate information. Section 623(a)(2).

### **Duties After Notice of Dispute from Consumer**

If a consumer notifies a furnisher, at an address specified by the furnisher for such notices, that specific information is inaccurate, and the information is, in fact, inaccurate, the furnisher must thereafter report the correct information to CRAs. Section 623(a)(1)(B).

If a consumer notifies a furnisher that the consumer disputes the completeness or accuracy of any information reported by the furnisher, the furnisher may not subsequently report that information to a CRA without providing notice of the dispute. Section 623(a)(3).

Furnishers must comply with federal regulations that identify when an information furnisher must investigate a dispute made directly to the furnisher by a consumer. Under these regulations, furnishers must complete an investigation within 30 days (or 45 days, if the consumer later provides relevant additional information) unless the dispute is frivolous or irrelevant or comes from a "credit repair organization." The CFPB regulations will be available at [consumerfinance.gov](http://consumerfinance.gov). Section 623(a)(8).

### **Duties After Notice of Dispute from Consumer Reporting Agency**

If a CRA notifies a furnisher that a consumer disputes the completeness or accuracy of information provided by the furnisher, the furnisher has a duty to follow certain procedures. The furnisher must:

- Conduct an investigation and review all relevant information provided by the CRA, including information given to the CRA by the consumer. Sections 623(b)(1)(A) and (b)(1)(B).
- Report the results to the CRA that referred the dispute, and, if the investigation establishes that the information was, in fact, incomplete or inaccurate, report the results to all CRAs to which the furnisher provided the information that compile and maintain files on a nationwide basis. Sections 623(b)(1)(C) and (b)(1)(D).
- Complete the above steps within 30 days from the date the CRA receives the dispute (or 45 days, if the consumer later provides relevant additional information to the CRA). Section 623(b)(2).
- Promptly modify or delete the information, or block its reporting. Section 623(b)(1)(E).

### **Duty to Report Voluntary Closing of Credit Accounts**

If a consumer voluntarily closes a credit account, any person who regularly and in the ordinary course of business furnishes information to one or more CRAs must report this fact when it provides information to CRAs for the time period in which the account was closed. Section 623(a)(4).

### **Duty to Report Dates of Delinquencies**

If a furnisher reports information concerning a delinquent account placed for collection, charged to profit or loss, or subject to any similar action, the furnisher must, within 90 days after reporting the information, provide the CRA with the month and the year of the commencement of the delinquency that immediately preceded the action, so that the agency will know how long to keep the information in the consumer's file. Section 623(a)(5).

Any person, such as a debt collector, that has acquired or is responsible for collecting delinquent accounts and that reports information to CRAs may comply with the requirements of Section 623(a)(5) (until there is a consumer dispute) by reporting the same delinquency date previously reported by the creditor. If the creditor did not report this date, they may comply with the FCRA by establishing reasonable procedures to obtain and report delinquency dates, or, if a delinquency date cannot be reasonably obtained, by following reasonable procedures to ensure that the date reported precedes the date when the account was placed for collection, charged to profit or loss, or subjected to any similar action. Section 623(a)(5).

### **Duties of Financial Institutions When Reporting Negative Information**

Financial institutions that furnish information to "nationwide" consumer reporting agencies, as defined in Section 603(p), must notify consumers in writing if they may furnish or have furnished negative information to a CRA. Section 623(a)(7). The CFPB has prescribed model disclosures, 12 CFR Part 1022, App. B.

### **Duties When Furnishing Medical Information**

A furnisher whose primary business is providing medical services, products, or devices (and such furnisher's agents or assignees) is a medical information furnisher for the purposes of the FCRA and must notify all CRAs to which it reports of this fact. Section 623(a)(9). This notice will enable CRAs to comply with their duties under Section 604(g) when reporting medical information.

### **Duties when ID Theft Occurs**

All furnishers must have in place reasonable procedures to respond to notifications from CRAs that information furnished is the result of identity theft, and to prevent refurnishing the information in the future. A furnisher may not furnish information that a consumer has identified as resulting from identity theft unless the furnisher subsequently knows or is informed by the consumer that the information is correct. Section 623(a)(6). If a furnisher learns that it has furnished inaccurate information due to identity theft, it must notify each CRA of the correct information and must thereafter report only complete and accurate information. Section 623(a)(2). When any furnisher of information is notified pursuant to the procedures set forth in Section 605B that a debt has resulted from identity theft, the furnisher may not sell, transfer, or place for collection the debt except in certain limited circumstances. Section 615(f).

The CFPB's website, [consumerfinance.gov/learnmore](http://consumerfinance.gov/learnmore), has more information about the FCRA, including publications for businesses and the full text of the FCRA.

### **Citations for FCRA sections in the U.S. Code, 15 U.S.C. § 1681 et seq.:**

Section 602	15 U.S.C. 1681	Section 615	15 U.S.C.1681m
Section 603	15 U.S.C. 1681a	Section 616	15 U.S.C. 1681n
Section 604	15 U.S.C. 1681b	Section 617	15 U.S.C. 1681o
Section 605	15 U.S.C. 1681c	Section 618	15 U.S.C. 1681p
Section 605A	15 U.S.C. 1681cA	Section 619	15 U.S.C. 1681q
Section 605B	15 U.S.C. 1681cB	Section 620	15 U.S.C. 1681r
Section 606	15 U.S.C. 1681d	Section 621	15 U.S.C. 1681s
Section 607	15 U.S.C. 1681e	Section 622	15 U.S.C. 1681s-1
Section 608	15 U.S.C. 1681f	Section 623	15 U.S.C. 1681s-2
Section 609	15 U.S.C. 1681g	Section 624	15 U.S.C. 1681t
Section 610	15 U.S.C. 1681h	Section 625	15 U.S.C. 1681u
Section 611	15 U.S.C. 1681i	Section 626	15 U.S.C. 1681v
Section 612	15 U.S.C. 1681j	Section 627	15 U.S.C. 1681w
Section 613	15 U.S.C. 1681k	Section 628	15 U.S.C. 1681x
Section 614	15 U.S.C. 1681l	Section 629	15 U.S.C. 1681y



# Know Your Rights

If someone steals your identity, you have the right to:

- Create an Identity Theft Report.
- Place a one-year fraud alert on your credit report.
- Place a seven-year extended fraud alert on your credit report.
- Get free copies of your credit report.
- Get fraudulent information removed (or blocked) from your credit report.
- Dispute fraudulent or inaccurate information on your credit report.
- Stop creditors and debt collectors from reporting fraudulent accounts.
- Get copies of documents related to the identity theft.
- Stop a debt collector from contacting you.

## Documenting the Theft

You have the right to:

- Create an **Identity Theft Report**. Your Identity Theft Report helps prove to businesses that someone stole your identity, and makes it easier to correct problems caused by identity theft. You can create an Identity Theft Report by filing a report with the FTC at **IdentityTheft.gov**.

## Working with Credit Bureaus

You have the right to:

- Place a **one-year fraud alert** on your credit report. The fraud alert tells creditors that they must take reasonable steps to verify who is applying for credit in your name. To place this alert, contact one of the three national credit bureaus: Equifax, TransUnion, or Experian. The one you contact must notify the others.

When you place a fraud alert, you're also entitled to a free copy of your credit reports. You'll get a confirmation letter from each credit bureau with instructions for how to get your free reports.

- Place a **seven-year extended fraud alert** on your credit report. To do this, send a copy of your Identity Theft Report to one credit bureau. That one must tell the other two. The extended fraud alert means potential creditors must contact you before they issue credit in your name. In your letter, be sure to give the best way for a creditor to reach you.

- Each credit bureau will send you a letter confirming that they placed an extended fraud alert on your file. That letter also will include instructions about how to get free copies of your credit report.
- **Get credit bureaus to remove fraudulent information from your credit report.** This is called blocking. You must send them a copy of your Identity Theft Report, proof of your identity, and a letter stating which information is fraudulent. Then the credit bureau must tell the relevant creditor that someone stole your identity. Creditors cannot turn fraudulent debts over to debt collectors. There's a sample letter on page 20.
- **Dispute fraudulent or inaccurate information on your credit report.** Do this by writing to the credit bureau. They must investigate your dispute and amend your report if it is fraudulent or inaccurate.
- You have the right to **place a freeze on your credit report.** A credit freeze, also called a security freeze, makes it less likely that an identity thief could open a new account in your name.

## Communicating with Creditors and Debt Collectors

You have the right to:

- **Stop creditors and debt collectors from reporting fraudulent accounts.** After you give them a copy of a valid Identity Theft Report, they may not report fraudulent accounts to the credit bureaus. There's a sample letter on page 21.
- **Get copies of documents related to the theft of your identity,** like transaction records or applications for new accounts. Write to the company that has the documents, and include a copy of your Identity Theft Report. You also can tell the company to give the documents to a specific law enforcement agency.
- **Stop a debt collector from contacting you.** In most cases, debt collectors must stop contacting you after you send them a letter telling them to stop.
- **Get written information from a debt collector about a debt,** including the name of the creditor and the amount you supposedly owe. If a debt collector contacts you about a debt, request this information in writing.

## Limits on Financial Losses

You have limited liability for fraudulent debts caused by identity theft.

- Under most state laws, you're not responsible for any debt incurred on **fraudulent new accounts** opened in your name without your permission.
- Under federal law, the amount you have to pay for unauthorized use of your **credit card** is limited to \$50. If you report the loss to the credit card company before your credit card is used by a thief, you aren't responsible for any unauthorized charges.



- If your **ATM or debit card** is lost or stolen, you can limit your liability by reporting the loss immediately to your bank or credit union.

If you report your debit card lost:	Your maximum loss is:
Before any unauthorized charges are made	\$0
Within 2 business days after you learn about the loss or theft	\$50
More than 2 business days after you learn about the loss or theft, but less than 60 calendar days after your statement is sent to you	\$500
More than 60 calendar days after your statement is sent to you	Possibly unlimited

- If someone makes unapproved debits to your bank or credit union account using your **debit card number** (not your card), you aren't responsible – as long as you report the problem within 60 days of the statement with the fraudulent debits.
- Most state laws limit your liability for **fraudulent checks** issued on your bank or credit union account if you notify the bank or credit union promptly.

### Other Federal Rights

Under the Justice for All Act, you have additional rights when the identity thief is **criminally prosecuted in federal court**. You have the right to:

- Reasonable protection from the accused.
- Reasonable, accurate, and timely notice about any related public court or parole proceeding, or the release or escape of the accused.
- Not be excluded from any public court proceeding unless the judge decides that your testimony would change significantly if you heard other testimony.
- Be reasonably heard at any public proceeding in the district court that involves release, plea, sentencing, or parole.
- Confer with the attorney for the government in the case.
- Full and timely restitution, as provided in the law proceedings, free from unreasonable delay.
- Be treated with fairness and respect for your dignity and privacy.

### State Rights

In many states, businesses or organizations that lose or misplace certain types of personal information must tell you if that has happened. To learn more, check with your state and local consumer protection offices, which you can find at [usa.gov/state-consumer](http://usa.gov/state-consumer).

# Data Breaches and Lost or Stolen Info

Did you recently get a notice that says your personal information was exposed in a data breach? Did you lose your wallet? Or learn that an online account was hacked? Did a company contact you because someone tried to open a credit card in your name?

Going forward, it's important to monitor your credit report and your accounts. If you find accounts or charges that you don't recognize, read [What To Do Right Away](#) on page 1.

Depending on what information was lost or stolen, there are steps you can take to help protect yourself from identity theft.

## Social Security Number

- ☐ If a company responsible for exposing your information offers you free credit monitoring, take advantage of it.
- ☐ Get your free credit reports from [annualcreditreport.com](https://annualcreditreport.com). Check for any accounts or charges you don't recognize.
- ☐ Consider placing a credit freeze. A credit freeze makes it harder for someone to open a new account in your name.

If you place a freeze, be ready to take a few extra steps the next time you apply for a new credit card or cell phone – or any service that requires a credit check.

If you decide not to place a credit freeze, at least consider placing a fraud alert.

- ☐ Try to file your taxes early – before a scammer can. Tax identity theft happens when someone uses your Social Security number to get a tax refund or a job. Respond right away to letters from the IRS.
- ☐ Don't believe anyone who calls and says you'll be arrested unless you pay for taxes or debt – even if they have part or all of your Social Security number, or they say they're from the IRS.
- ☐ Continue to check your credit reports at [annualcreditreport.com](https://annualcreditreport.com). You can order a free report from each of the three credit bureaus once a year.



## Online Login or Password

- ☐ Log in to that account and change your password. If possible, also change your username.

If you can't log in, contact the company. Ask them how you can recover or shut down the account.

- ☐ If you use the same password anywhere else, change that, too.
- ☐ Is it a financial site, or is your credit card number stored? Check your account for any charges that you don't recognize.

## Debit or Credit Card Number

- ☐ Contact your bank or credit card company to cancel your card and request a new one.
- ☐ Review your transactions regularly. Make sure no one misused your card.

If you find fraudulent charges, call the fraud department and get them removed.

- ☐ If you have automatic payments set up, update them with your new card number.
- ☐ Check your credit report at **annualcreditreport.com**.

## Bank Account Information

- ☐ Contact your bank to close the account and open a new one.
- ☐ Review your transactions regularly to make sure no one misused your account.

If you find fraudulent charges or withdrawals, call the fraud department and get them removed.

- ☐ If you have automatic payments set up, update them with your new bank account information.
- ☐ Check your credit report at **annualcreditreport.com**.

## Driver's License Information

- ☐ Contact your nearest motor vehicles branch to report a lost or stolen driver's license. The state might flag your license number in case someone else tries to use it, or they might suggest that you apply for a duplicate.

- ☐ Check your credit report at [annualcreditreport.com](https://annualcreditreport.com).

## Children's Personal Information

- ☐ Check to see if your child has a credit report. See page 14 for instructions on how to do so.

If a credit bureau has a credit report for your child, the credit bureau will send you a copy of the report. Use the instructions provided with the credit report to remove the fraudulent accounts.

- ☐ Contact each credit bureau and request a credit freeze for your child. A credit freeze will make it difficult for someone to use your child's information to open accounts. To place a freeze, follow the specific instructions for each credit bureau.
  - **Experian.com/help**  
888-EXPERIAN (888-397-3742)
  - **TransUnion.com/credit-help**  
888-909-8872
  - **Equifax.com/personal/credit-report-services**  
800-685-1111

Get updates at [IdentityTheft.gov/creditbureaucontacts](https://IdentityTheft.gov/creditbureaucontacts).

- ☐ Review the FTC's information on Child Identity Theft at [consumer.ftc.gov/childidt](https://consumer.ftc.gov/childidt).



TransUnion<sup>tu</sup>



