

IDENTITY THEFT

Recovering from Identity Theft

Is someone using your personal information to open accounts, file taxes, or make purchases?

Visit IdentityTheft.gov, the federal government's one-stop resource to help you report and recover from identity theft.



Data Breach? Lost Info?



Did you get a notice that says a company lost your personal information in a data breach? Did you lose your wallet? Or learn that an online account was hacked? Here are [steps you can take](#) to help protect yourself from identity theft.

Protecting Your Identity



What can you do to keep your personal info secure? Are identity protection services worth the cost? What about credit freezes? Check out the [FTC's identity theft articles](#) to find out.

Free Resources for Your Community



You can help people learn about identity theft — whether you're chatting with friends and family, sharing info on a social networking site, or taking resources to a religious group or PTA meeting. It's easy to use and share these free resources from the FTC.

- [Free Identity Theft Resources](#)
Free booklets —in English and Spanish — to help people in your community learn how to protect their identity and recover if an identity thief strikes
- [Protect Your Identity Event Kit](#)
Everything you need to plan and host an event about identity theft
- [Identity Theft Videos](#)
Three videos —in English and Spanish — that explain what identity theft is, how to spot it, and how to recover

For Law Enforcement



Local police can help identity theft victims by:

- helping them file a police report
- sharing [free identity theft resources from the FTC](#)

Credit bureaus and other businesses often require that identity theft victims provide a police report to remove fraudulent debts. Please share our [memo to law enforcement](#) with fellow officers so they understand how they can help.

For Attorneys and Advocates



The [FTC's Guide for Assisting Identity Theft Victims](#) is designed to assist attorneys who counsel identity theft victims. The guide highlights the rights and remedies available to identity theft victims under federal law, and provides other useful resources, like sample letters.

For Businesses



Many companies keep sensitive information about customers or employees in their files or on their network. The FTC has [free data security resources](#) — including free publications, videos, and tutorials — to help businesses of any size protect their customers and meet their legal obligations.



What To Do Right Away

Did someone steal and use your personal information? Act quickly to limit the damage.

▼ 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 report.

- Contact one of the three credit bureaus. That company must tell the other two.

- [Equifax.com/CreditReportAssistance](https://www.equifax.com/CreditReportAssistance) 
[1-888-766-0008](tel:1-888-766-0008)
- [Experian.com/fraudalert](https://www.experian.com/fraudalert) 
[1-888-397-3742](tel:1-888-397-3742)
- [TransUnion.com/fraud](https://www.transunion.com/fraud) 
[1-800-680-7289](tel:1-800-680-7289)

A fraud alert is free. 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 report right away. Go to annualcreditreport.com  or call [1-877-322-8228](tel: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 each fraud alert confirmation

letter to get a free report, but it 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 FTC and the police.

▼ Step 3: Report identity theft to the FTC.

- Complete the FTC's [online complaint form](#). Give as many details as you can. The complaint form is not available on mobile devices, but you can call [1-877-438-4338](tel:1-877-438-4338) to make your report.

Based on the information you enter, the FTC complaint system will create your Identity Theft Affidavit. You'll need this to complete other steps.

- Print** and **save** your FTC Identity Theft Affidavit immediately. Once you leave the page, you won't be able to get your affidavit.

Do you need to update your affidavit? Call [1-877-438-4338](tel:1-877-438-4338).

▼ Step 4: File a report with your local police department.

- Go to your local police office with:
 - a copy of your FTC Identity Theft Affidavit
 - 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, IRS notices, etc.)
 - [FTC's Memo to Law Enforcement \[PDF\]](#)
- Tell the police someone stole your identity and you need to file a report. If they are reluctant, show them the [FTC's Memo to Law Enforcement \[PDF\]](#).
- Ask for a copy of the police report. You'll need this to complete other steps.
- Create your Identity Theft Report by combining your FTC Identity Theft Affidavit with your police report.



Your identity theft report proves to businesses that someone stole your identity. It also guarantees you certain rights.



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. This [sample letter](#) 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 them.
 - Ask the business to send you a letter confirming they removed the fraudulent charges.
 - Keep this letter. Use it if this 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. This [sample letter](#) can help.

- Write down who you contacted and when.
-

▼ Correct your credit report.

-
- ❑ Write to each of the three credit bureaus. This [sample letter](#) can help.
 - Include a copy of your Identity Theft Report and proof of your identity, like your name, address, and Social Security number.
 - Explain which information on your report came from identity theft.
 - Ask them to block that information.
 - [Equifax.com](#) 
 - P.O. Box 105069
 - Atlanta, GA 30348-5069
 - [1-800-525-6285](tel:1-800-525-6285)
 - [Experian.com](#) 
 - P.O. Box 9554
 - Allen, TX 75013
 - [1-888-397-3742](tel:1-888-397-3742)
 - [TransUnion.com](#) 
 - Fraud Victim Assistance Department
 - P.O. Box 2000
 - Chester, PA 19022-2000
 - [1-800-680-7289](tel:1-800-680-7289)

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 this 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.

▼ Consider adding an extended fraud alert or credit freeze.

Extended Fraud Alert	Credit Freeze
Lets you have access to your credit report as long as companies take steps to verify your identity	Stops all access to your credit report unless you lift or remove it
Free to place and remove if someone stole your identity. Guaranteed by federal law.	Cost and availability depend on your state law  . There might be a small fee for placing, lifting and removing.
Lasts for 7 years	Lasts until you lift or remove

<p>Set it by contacting each of the three credit bureaus:</p> <ol style="list-style-type: none"> 1. Report that someone stole your identity. Request an extended fraud alert. 2. Complete any necessary forms and send a copy of your Identity Theft Report. 	<p>Set it by contacting each of the 3 credit bureaus.</p> <ol style="list-style-type: none"> 1. Report that someone stole your identity. 2. Ask the company to put a freeze on your credit file. 3. Pay the fee required by state law
<p>For fraud alerts:</p> <ul style="list-style-type: none"> • TransUnion.com  1-800-680-7289 • Experian.com  1-888-397-3742 • Equifax.com  1-888-766-0008 	<p>For credit freezes:</p> <ul style="list-style-type: none"> • TransUnion.com  1-888-909-8872 • Experian.com  1-888-397-3742 • Equifax.com  1-800-349-9960

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.

Other Steps

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

Resolve tax-related identity theft.

If you get an IRS notice in the mail, follow the instructions provided.

Complete [IRS Form 14039, Identity Theft Affidavit \[PDF\]](#). Mail or fax the form according to the instructions. Include proof of your identity, like a copy of your Social Security card, driver's license or passport.

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.

If these steps don't resolve your situation, contact the IRS for specialized assistance at [1-800-908-4490](tel:1-800-908-4490).

Report a misused Social Security number.

Social Security card lost or stolen? [Apply online](#) for free to get a replacement card.

Do you think someone else is using your Social Security number for work? Review your Social Security work history by creating an account at socialsecurity.gov/myaccount. If you find errors, contact your [local 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. This [sample letter](#) 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. This [sample letter](#) can help.

For example, if someone opened a credit card in your name, ask for a copy of the application and 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](#)" can help you block fraudulent information from your credit reports.

Write down who you contacted and when. Keep copies of any letters you send.

Replace government-issued IDs.

Social Security card lost or stolen? [Apply online](#) for **free** to get a replacement card.

Driver's license lost or stolen? Contact the [nearest DMV branch](#) to report it.

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](tel:1-877-487-2778) or TTY [1-888-874-7793](tel: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 \[PDF\]](#) and [DS-64 \[PDF\]](#) in person at an authorized [Passport Application Acceptance Facility](#).

Resolve child identity theft.

Follow the usual steps for [What To Do Right Away](#) and [What To Do Next](#) with 2 exceptions:

- When requesting a credit report, ask for a search based only on your child's Social Security number (SSN). You'll need to do this by phone or email:
 - **Equifax**
[1-800-525-6285](tel:1-800-525-6285)
 - **Experian**
[1-888-397-3742](tel:1-888-397-3742)
 - **TransUnion.com**
childidtheft@transunion.com
- When you correct your child's credit report, send each credit reporting agency the [Minor's Status Declaration \[PDF\]](#) form. It provides proof that your child is a minor. Include a letter with the form that asks for all information associated with your child's name or SSN to be removed. If you do this, you don't have to send a "blocking" request for the child.

The SSN-only search means that any items associated with your child's SSN are included in the report -- even if the thief used your child's SSN with a different name.

Because a minor cannot legally agree to contracts, any debts on your child's credit report are fraudulent by definition.

Resolve medical identity theft.

If you think a thief used your personal information to get medical services, get copies of your 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](#).

Review your medical records, and 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 3 credit reporting companies](#).

Write down who you contacted and when. Keep copies of any letters you send.

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](#).

- 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. The [American Bar Association](#) or a local [legal services provider](#) 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.

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

Utilities

Did an identity thief open a new account to get telephone, cable, electric, water, or other similar services in your name? Contact the service provider.

- Tell them someone stole your identity.
- Ask them to close the account.

For additional help, contact your [state Public Utility Commission](#) and explain the situation.

For help with cell phone or telephone service, contact the [Federal Communications Commission](#) at 1-888-225-5322 or TTY 1-888-835-5322.

Write down who you contacted and when. Keep copies of any letters you send.

Checking accounts

Do you think someone opened a new 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](#). Or visit their website [consumerdebit.com](#).
- 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 its check verification system. The check verification system will tell businesses to refuse the stolen checks.

- Also, contact any business that took the bad check. Explain that someone stole your identity theft. 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](tel:1-800-710-9898)

Certegy [1-800-437-5120](tel:1-800-437-5120)

If a business rejects your checks, 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.

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.

Contact the [U.S. Department of Education](#) at [1-800-647-8733](tel:1-800-647-8733).

If these steps don't resolve your situation, contact the U.S. Department of Education Ombudsmen at [202-277-3800](tel:202-277-3800) or [online](#).

Write down who you contacted and when. Keep copies of any letters you send.

Investment accounts

Call your broker or account manager, and describe the situation.

[File a complaint](#) with the Securities and Exchange Commission (SEC).

For more information, you can call the SEC at [1-800-732-0330](tel:1-800-732-0330).

Write down who you contacted and when. Keep copies of any letters you send.

Bankruptcy filed in your name

Write to the [U.S. Trustee](#) in the region where the bankruptcy was filed. Describe the situation and 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. The [American Bar Association](#) or a local [legal services provider](#) 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.