Table of Contents

Has Someone Stolen Your Identity? You Aren’t Alone.

Para ver este artículo en español por favor visite aquí. (To view this article in Spanish, visit here.)

Millions of individuals fall victim to identity theft each year, leading to significant emotional and financial distress. The rise of digital transactions and online services has made it easier for criminals to access personal information, often without the victim's knowledge. Sometimes this is not something that you yourself can easily prevent. Your personal data can be stolen from or leaked by large companies. Thieves can then get a hold of this personal data and use it to impersonate you.

What is Identity Theft?

Identity theft occurs when someone steals your identity to commit fraud. Federal Trade Commission data shows that in 2023, there were 917,315 identity theft reports in the United States. Identity theft happens in a variety of ways. Common methods include:

- phishing, where scammers impersonate legitimate organizations to trick individuals into providing sensitive information;
- data breaches, where cyberattacks on companies lead to stolen personal data; and
- skimming, where devices capture card information at ATMs or point-of-sale systems.

Mail theft, social engineering tactics, vulnerabilities in public Wi-Fi networks, and fake websites also pose significant risks.

When someone steals your identity to commit fraud, it means that someone is using your personal information without your permission, such as:

- Your name
- Social Security or Medicare number
- Credit card number
- Address
- Date of birth

Identity thieves may rent apartments, get credit cards, receive government benefits or tax refunds, or open other accounts in your name. It's possible that you may not find out about the identity theft until you review your credit report or a credit card statement and notice accounts you didn't open, charges you didn't make, or until you're contacted by a debt collector. Am I at risk of identity theft?

Identity theft can happen to anyone. The more information you provide readily available online, however, including information about your children, such as publicly sharing your child's birth date and full name, can make it easier for criminals to steal an identity.

Here are some ways you can protect your personal information:

- Store personal information securely in a safe place. Shred documents before you throw them away.
- Don't share your social security number with someone who contacts you. Legitimate organizations that might need your social security number typically do not reach out to you first. Also, do not provide your social security number in online job applications. Wait until you have an offer and verify that the company is legitimate.
- Protect your information online and on your phone. Make sure to use a password. Strong passwords have:
    - At least 12 characters. Try using a phrase or combination of words that makes sense only to you.
    - A combination of upper and lower case letters, numbers, and special characters
    - Do not use personal information
    - Keep social media accounts private. If you are an influencer or choose to publicly share your social media, be careful with how much information

you share, especially information about any minor children.
    - It is also important to use different, unique passwords for different websites and needs. One way you can do this is by loosely associating the account type with a password.
- For example, if you have an account with a grocery store and your favorite type of produce is apples, specifically honey crisp apples, and you started going to this grocery store in 2019, then your password might be HONEYcrispEATER2019!
    - If you have an account with a local bank and you use this bank account to pay your car loans for your 2014 Toyota Camery, and the bank's logo color is navy, your password might be navyTOYOTAdriver2014$
    - Avoid using birthdays, names of family members, including pets, default passwords, or common passwords such as "password" or "12345678"

If you've been a victim of identity theft, visit IdentityTheft.gov, the federal government's one-stop resource to help you report and recover from identity theft. IdentityTheft.gov allows you to report identity theft, while also receiving an Identity Theft Report and a personal recovery plan that walks you through the steps to take. For example, you can contact the nationwide credit reporting companies for help with placing fraud alerts or security freezes and blocking or removing fraudulent debts.

Credit Fraud Alerts and Credit Freezes

You do not have to be a victim of identity theft to place fraud alerts or security freezes on your account.

A credit fraud alert and a credit freeze are both important tools designed to protect consumers from identity theft, but they serve different purposes and operate in distinct ways. A credit fraud alert is a notification placed on your credit report that warns potential creditors to take extra steps to verify your identity before granting credit. Typically lasting for 90 days, a fraud alert can be extended and is initiated through one of the three major credit bureaus—Equifax, Experian, or TransUnion. When you place a fraud alert, the bureau will notify the others. Importantly, a fraud alert does not impact your credit score; it simply serves as a precautionary measure for creditors.

In contrast, a credit freeze restricts access to your credit report, making it impossible for new creditors to access your information without your consent. A freeze can be placed and lifted at any time, allowing you full control over when your credit report is accessible. Like a fraud alert, a credit freeze does not affect your credit score, as it prevents unauthorized access but doesn't impact existing accounts or your credit utilization.

If you decide to apply for a loan or any other credit, you can temporarily lift a credit freeze. This can be done online, by phone, or by mail, depending on the credit bureau. You will need to provide the PIN or password associated with the freeze to lift it. The PIN or password will be either set by you or the credit reporting agency will sent you a copy. For example, if you call Equifax and tell them you want to freeze your credit, Equifax would set a randomly-generated password for your credit freeze. If you want to unfreeze your credit with Equifax, you will have to provide that same password.

In summary, while both credit fraud alerts and credit freezes help protect against identity theft, they function differently. A fraud alert encourages creditors to verify identity, while a credit freeze completely restricts access to your credit report. Neither action affects your credit score, and a credit freeze can be lifted temporarily when you apply for a loan, credit card, or change bank accounts.

Steps to Take

The "Steps" Section of IdentityTheft.gov has conveniently laid out steps on what to do if you fall victim to tax, medical, or child identity theft:

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.

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

- Place a free, one-year fraud alert by contacting one of the three credit bureaus. That company must tell the other two.

Online	By calling	By mail
Equifax Alerts	(800) 685-1111	Equifax Consumer Fraud Division, P.O. Box 740256, Atlanta, GA 30374
Experian Fraud Center	(888) 397-3742	Experian, P.O. Box 9554, Allen, TX 75013
Transunion Fraud Alert	(888) 909-8872	TransUnion Fraud Victim Assistance Department, P.O. Box 2000, Chester, PA 19016

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

Step 3 - Report identity theft to the FTC.

- Complete the online form or call 1-877-438-4338. Include as many details as possible.
- If you create an account, the FTC will 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.

You may additionally choose to file a report with your local police department:

- 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, 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. You may need this to complete other steps.

Blocking or removing fraudulent information from your consumer report

If you've been a victim of identity theft, you can also ask credit reporting companies to remove fraudulent information and debts from your credit report, which is called blocking. To do this, you must send the credit reporting companies:

- An identity theft report, which can be done through IdentityTheft.gov
- Proof of your identity
- A letter identifying the fraudulent debts and information on your credit report

Through IdentityTheft.gov, you can also get a sample letter to send to the credit reporting companies. Remember that you can use identity theft reports only for debts that are the result of identity theft. Credit reporting companies may decline to block or rescind a block if you make a material misrepresentation of fact about being a victim of identity theft or if you got goods, services, or money as a result of the blocked transaction.

Within four business days after receiving your request, the credit reporting company must block that information from your credit report. In addition, they must tell the companies that provided the information that someone stole your identity. Once notified, creditors can't turn identity theft-related debts over to debt collectors.

If you need to dispute a debt that is not the result of identity theft, read "How do I dispute an error on my credit report?"

If you have a problem with credit reporting, you can submit a complaint to the CFPB.

More About Fraud Alerts and Freezes

As a brief reminder, a fraud alert requires creditors, who check your credit report, to take steps to verify your identity before they open a new account, issue an additional card, or increase the credit limit on an existing account based on a consumer's request. When you place a fraud alert on your credit report at one of the nationwide credit reporting companies, it must notify the others.

There are two main types of fraud alerts: initial fraud alerts and extended alerts. Servicemembers also have the option of an active-duty alert.

Initial Fraud Alerts

You can place an initial fraud alert on your credit report if you believe you are, or are about to become, a victim of fraud or identity theft. Credit reporting companies will keep that alert on your file for one year. After one year, the initial fraud alert will expire and be removed. You have the option to place another fraud alert at that time.

When you place an initial fraud alert, creditors must take reasonable steps to make sure the person making a new credit request in your name is you before granting that request. If you provide a telephone number, the creditor must call you or take reasonable steps to verify whether you are the person making the credit request before granting the credit.

When you place an initial fraud alert on your file, you're entitled to order one free copy of your credit report from each of the nationwide credit reporting companies. These free reports do not count as your free annual report from each credit reporting company.

If your identity has been stolen and you have filed an identity theft report at IdentityTheft.gov, you can place an extended alert on your credit report.

Extended Alert

An extended alert is good for seven years. If you have an extended alert, a creditor must contact you in person, on the telephone, or through another contact method you choose to verify if you are the person making the credit request before extending new credit.

When you place an extended fraud alert on your file, you're entitled to order two free copies of your credit report from each nationwide credit reporting company over a 12- month period. Your name will also be removed for five years from the nationwide credit reporting companies' pre-screen marketing lists for credit offers and insurance.

Active-duty Alerts

Servicemembers in the armed forces have an additional option available to them: active-duty alerts, which protect service members while they are on active duty and assigned away from their usual duty station. This alert requires businesses to take reasonable steps to verify your identity before issuing credit in your name. These

alerts last for 12 months, unless you request that the alert be removed sooner. If your deployment lasts longer than 12 months, you may place another alert on your credit file.

When you place an active-duty alert on your credit report, creditors must take reasonable steps to make sure the person making the request is you before they open an account, issue an additional credit card on an existing account, or increase the credit limit on your existing account. Your name will also be removed for two years from the nationwide credit reporting companies' pre-screen marketing lists for credit offers and insurance.

Since it may be very difficult to contact you directly if you are deployed, you can assign a personal representative to answer for you, or to place or remove an active-duty alert.

This article was compiled from sources such as the Consumer Finance Protection Bureau and the Federal Trade Commission, and edited by LawNY.

Consumer Financial Protection Bureau

* * * * *

Last Review Date: November 2024

Last updated on September 17, 2025.

Consumer
Article Legal Information

Print

Print

Table of Contents

NEWS

News & publications

More News

October 31, 2025

SNAP Benefit Update as of October 31, 2025

SNAP benefits for November 2025 may be delayed.The New York State Office of...

Read More about SNAP Benefit Update as of October 31, 2025

September 16, 2025

LawNY® in the News

2025 -Nursing home residents and families learn about their rights - News10ABC ...

Read More about LawNY® in the News

Our Partners

We proudly receive support from the following (to read a full list of our supporters, visit the "Who We Are" tab above):