



Securing today
and tomorrow

Identity Theft and Your Social Security Number



[SSA.gov/myaccount](https://ssa.gov/myaccount)

[SSA.gov](https://ssa.gov)



Identity theft is one of the fastest growing crimes in America. Scammers use your Social Security number (SSN) to get other personal information about you. They can use your SSN and your good credit to apply for more credit in your name. Then, when they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your SSN until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought.

Your SSN is confidential

We protect your SSN and keep your records confidential. We don't give your number to anyone, except when authorized by law. You should be careful about sharing your number, even when you're asked for it. You should ask why your number is needed, how it'll be used, and what will happen if you refuse. The answers to these questions can help you decide if you want to give out your SSN.

How might someone steal your SSN?

Scammers get your personal information by:

- Stealing wallets, purses, and your mail (bank and credit card statements, pre-approved credit offers, new checks, and tax information).

- Stealing personal information you provide to an unsecured site online, from business or personnel records at work, and personal information in your home.
- Rummaging through your trash, the trash of businesses, and public trash dumps for personal data.
- Buying personal information from “inside” sources. For example, a scammer may pay a store employee for information about you that appears on an application for goods, services, or credit.
- Posing by phone, email, text, or direct messages in social media as someone who legitimately needs information about you, such as employers, landlords, or government agencies.

Be careful with your SSN card

When you start a job, make sure your employer has your correct number to ensure your records are correct. Provide your SSN to your financial institution(s) for tax reporting purposes. Keep your card and any other document that shows your SSN in a safe place. Do not routinely carry your card or other documents that display your number.

What if you think someone is using your number?

Sometimes more than one person uses the same SSN, either on purpose or by accident. If you suspect someone is using your number for work purposes, you should report the problem to us. We'll review your earnings with you to ensure our records are correct.

You may also visit

www.ssa.gov/myaccount to sign in to or create a personal *my* Social Security account. With an online account, you can estimate your future benefits, and more.

What if a scammer is creating credit problems for you?

If someone has misused your SSN or other personal information to create credit or other problems for you, there are several things you can do.

- Visit **IdentityTheft.gov** to report identity theft and get a recovery plan. **IdentityTheft.gov** guides you through each step of the recovery process. It's a one-stop resource managed by the Federal Trade Commission, the nation's consumer protection agency. You can also call **1-877-IDTHEFT (1-877-438-4338)**; TTY **1-866-653-4261**.

- Contact the Internal Revenue Service (IRS). Scammers may also use your SSN to file a tax return to receive your refund. If you're eligible for a refund, a scammer could file a tax return before you do and get your refund. Then, when you do file, the IRS will think you already received your refund. If your SSN is stolen, another person may use it to get a job. That person's employer would report earned income to the IRS using your SSN. This makes it appear that you didn't report all of your income on your tax return. If you think you may have tax issues because someone has stolen your identity, go to **www.irs.gov/uac/Identity-Protection** or call **1-800-908-4490**.
- File an online complaint with the Internet Crime Complaint Center (IC3) at **www.ic3.gov**. The IC3 gives victims of cybercrime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. The IC3 sends every complaint to one or more law enforcement or regulatory agencies with jurisdiction.

The IC3's mission is to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cybercrime. The IC3 serves the broader law enforcement community that combats online crimes. This includes federal, state, local, and international agencies. The IC3

reflects a partnership between the Federal Bureau of Investigation, the National White Collar Crime Center, and the Bureau of Justice Assistance.

- You should also monitor your credit report periodically. You can get free credit reports online at ***www.annualcreditreport.com***.

Should you get a new SSN?

If you've done all you can to fix the problems resulting from misuse of your SSN, and someone is still using your number, we may assign you a new number.

You can't get a new SSN:

- If your SSN card is lost or stolen, but there's no evidence that someone is using your number.
- To avoid the consequences of filing for bankruptcy.
- If you intend to avoid the law or any legal responsibility.

If you decide to apply for a new number, you'll need to prove your identity, age, and U.S. citizenship or immigration status. For more information, ask for *Your Social Security Number and Card* (Publication Number 05-10002). You'll also need to provide evidence that you're having ongoing problems because of the misuse.

You should know that other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So, using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.

If you receive a new SSN, you shouldn't use the old number anymore.

For some victims of identity theft, a new number actually creates new problems. If the old credit information isn't associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit.

Contacting Us

The most convenient way to do business with us is to visit **www.ssa.gov** to get information and use our online services. There are several things you can do online: apply for benefits; start or complete your request for an original or replacement SSN card; get useful information; find publications; and get answers to frequently asked questions.

Or, you can call us toll-free at **1-800-772-1213** or at **1-800-325-0778** (TTY) if you're deaf or hard of hearing. We can answer your call from 8 a.m. to 7 p.m., weekdays. We provide free interpreter services upon request. For quicker access to a representative, try calling early in the day (between 8 a.m. and 10 a.m. local time) or later in the day. **We are less busy later in the week (Wednesday to Friday) and later in the month.** You can also use our automated services via telephone, 24 hours a day, so you do not need to speak with a representative.

Social Security Administration

Publication No. 05-10064

March 2026 (October 2024 editions may be used)

Identity Theft and Your Social Security Number

Produced and published at U.S. taxpayer expense