# Identity Theft, Prevention and Reporting Methods

Information gathered from www.usa.gov/identity-theft

Identity (ID) theft happens when someone steals your personal information to commit fraud.

The identity thief may use your information to fraudulently apply for credit, file taxes, or get medical services. These acts can damage your credit status, and cost you time and money to restore your good name.

You may not know that you're the victim of ID theft immediately. You could be a victim if you receive:

- Bills for items you didn't buy
- Debt collection calls for accounts you didn't open
- Denials for loan applications

Children and seniors are both vulnerable to ID theft. Child ID theft may go undetected for many years. Victims may not know until they're adults, applying for their own loans. Seniors are vulnerable because they share their personal information often with doctors and caregivers. The number of people and offices that access their information put them at risk.

## Types of ID Theft

There are several common types of identity theft that can affect you:

- Tax ID theft - Someone uses your Social Security number to falsely file tax returns with the IRS or your state
- Medical ID theft - Someone steals your Medicare ID or health insurance member number. Thieves use this information to get medical services or send fake bills to your health insurer.
- Social ID theft - Someone uses your name and photos to create a fake account on social media

Take steps to avoid being a victim of identity theft. Secure your internet connections, use security features, and review bills. Read more about how you can prevent identity theft.

## Steps to take to protect yourself from identity theft:

- Secure your Social Security number (SSN). Don't carry your Social Security card or birth certificate in your wallet. Only give out your SSN when absolutely necessary.
- Don't share personal information (birthdate, Social Security number, or bank account number) just because someone asks for it.
- Collect mail every day. Place a hold on your mail when you are away from home for several days.
- Pay attention to your billing cycles. If bills or financial statements are late, contact the sender.
- Use the security features on your mobile phone.
- Update sharing and firewall settings when you're on a public wi-fi network. Use a virtual private network, if you use public Wi-Fi.
- Review your credit card and bank account statements. Compare receipts with account statements. Watch for unauthorized transactions.
- Shred receipts, credit offers, account statements, and expired credit cards, to prevent "dumpster divers" from getting your personal information.
- Store personal information in a safe place.
- Install firewalls and virus-detection software on your home computer.
- Create complex passwords that identity thieves cannot guess. Change your passwords if a company that you do business with has a breach of its databases
- Review your credit reports once a year. Be certain that they don't include accounts that you have not opened. You can order it for free from Annualcreditreport.com.
- Freeze your credit files with Equifax, Experian, Innovis, TransUnion, and the National Consumer Telecommunications and Utilities Exchange, for free. Credit freezes prevent someone from applying for and getting approval for credit account or utility services in your name.

## Report Identity Theft

Report identity (ID) theft to the Federal Trade Commission (FTC) online at IdentityTheft.gov or by phone at 1-877-438-4338.

If you report identity theft online, you will receive an identity theft report and a recovery plan. Create an account on the website to update your recovery plan, track your progress, and receive prefilled form letters to send to creditors. If you don't create an account, you won't be able to access the report or letters later. Download the FTC's publication (PDF, Download Adobe Reader) for detailed tips, checklists, and sample letters.

If you report identity theft by phone, the FTC will collect the details of your situation. But it won't give you an ID theft report or recovery plan.

You may also choose to report your identity theft to your local police station. It could be necessary if:

- You know the identity thief
- The thief used your name in an interaction with the police
- A creditor or another company requires you to provide a police report.

## Report Specific Types of ID Theft

You may also report specific types of identity theft to other federal agencies.

- Medical Identity Theft - Contact Medicare's fraud office, if you have Medicare.
- Tax Identity Theft - Report tax ID theft to the Internal Revenue Service.

## Report ID Theft to other Organizations

You can also report the theft to other organizations, such as:

- Credit Reporting Agencies - Contact one of the three major credit reporting agencies to place fraud alerts or freezes on your accounts. Also get copies of your credit reports, to be sure that no one has already tried to get unauthorized credit accounts with your personal information. Confirm that the credit reporting agency will alert the other two credit reporting agencies.
- National Long-Term Care Ombudsman Resource Center - Report cases of identity theft that resulted from a stay in a nursing home or long-term care facility.
- Financial Institutions - Contact the fraud department at your bank, credit card issuers and any other places where you have accounts.
- Retailers and Other Companies - Report the crime to companies where the identity thief opened credit accounts or even applied for jobs.
- State Consumer Protection Offices or Attorney General - Some states offer resources to help you contact creditors and dispute errors.

You may need to get new personal records or identification cards if you're the victim of ID theft. Learn how to replace your vital identification documents after identity theft.

## Tax ID Theft

Tax-related identity theft occurs when someone uses your Social Security number to get a tax refund or a job. You may not be aware of the problem until you E-file your tax return and find out that another return has already been filed using your Social Security number. If the IRS suspects tax ID theft, they will send a 5071C letter to the address on the federal tax return. Keep in mind, the IRS will never start contact with you by sending an email, text, or social media message that asks for personal or financial information. Watch out for IRS imposter scams, when someone contacts you saying they work for the IRS.

### Report Tax ID Theft

- File a report with the Federal Trade Commission (FTC) at IdentityTheft.gov. You can also call the FTC Identity Theft Hotline at 1-877-438-4338 or TTY 1-866-653-4261.
- Contact one of the three major credit bureaus to place a fraud alert on your credit records:
    - Equifax: 1-888-766-0008
    - Experian: 1-888-397-3742
    - TransUnion: 1-800-680-7289
- Contact your financial institutions, and close any accounts opened without your permission or that show unusual activity.
- Respond immediately to any IRS notice; call the number provided. If instructed, go to the IRS Identity Verification Service.
- Complete IRS Form 14039, Identity Theft Affidavit (PDF, Download Adobe Reader); print, then mail or fax according to instructions.
- Continue to pay your taxes and file your tax return, even if you must do so by paper.
- Check with your state tax agency to see what steps to take at the state level.

## How to protect yourself from Tax Identity Theft

Follow these steps to prevent tax identity theft:

### Do

File your income taxes early in the season, before a thief can file taxes in your name. Also, Keep an eye out for any IRS letter or notice that states:

- More than one tax return was filed using your Social Security number.
- You owe additional tax, you have had a tax refund offset, or you have had collection actions taken against you for a year you did not file a tax return.
- IRS records indicate you received wages from an employer unknown to you.

### Don't

- Don't reply to or click on any links in suspicious email, texts, and social media messages. Make sure to report anything suspicious to the IRS.

## Medical ID Theft

Medical identity theft can occur when someone steals your personal identification number to obtain medical care, buy medication, access your medical records, or submit fake claims to your insurer or Medicare in your name.

## Report Medical ID Theft

If you believe you have been a victim of medical identity theft, call the Federal Trade Commission at 1-877-438-4338 (TTY: 1-866-653-4261) and your health insurance company's fraud department. You can report the theft through IdentityTheft.gov to share with the FTC and with law enforcement. Also get copies of your medical records and work with your doctor's office and insurance company to correct them.

If you suspect that you have been the victim of Medicare fraud, contact the U.S. Department of Health and Human Services' Inspector General at 1-800-447-8477.

## Prevent Medical ID Theft

Take these steps to prevent medical identity theft:

- Guard your Social Security, Medicare, and health insurance identification numbers. Only give your number to your physician or other approved health care providers.

- Review your explanation of benefits or Medicare Summary Notice to make sure that the claims match the services you received. Report questionable charges to your health insurance provider or Medicare.
- Request and carefully review a copy of your medical records for inaccuracies and conditions that you don’t have.