Neighborhood Watch

IDENTITY THEFT

Identity theft happens when someone uses information about you without your permission. An identity thief can use your name and information to buy things with your credit cards, get new credit cards, open accounts for phone, electric or gas, steal your tax refund, obtain medical care, or even pretend to be you if they are arrested.

Why should I care if someone steals my identity?

You may be responsible for what the thief does while using your personal information and/or you may have to pay for what the thief purchases. This is true even if you are not aware of the charges.

How can that happen?

A thief may get a credit card using your name. The thief would change the address on the account so the bills go to him, but he never pays them. That means the credit card company thinks you are not paying your bills and that will affect your credit.

How to protect yourself from identity theft

1. Freeze your credit

A credit freeze (or security freeze) is one of the most effective ways to prevent identity theft. Contact the three major credit bureaus individually to initiate the fraud alerts, credit freeze, and opt outs from pre-screened credit offers. When requesting a credit freeze online, the bureau may supply or have you create a personal identification number (PIN) or password to use when thawing or reactivating your freeze.

Equifax Equifax.com/personal/credit-report-services/ 800-685-1111

Experian Experian.com/freeze 888-EXPERIAN (888-397-3742)

TransUnion TransUnion.com/credit-freeze 888-909-8872

2. Monitor your accounts and reports

Regularly check your bank and credit card statements for unauthorized charges. If unauthorized charges are discovered, contact your banking institution immediately. Sign up to receive your statements online, to avoid theft from your mailbox.

Cancel credit cards you are not using. The fewer credit cards you have, the less you will have to monitor.

Get a copy of your credit report annually. Your credit report is a summary of your credit history. It lists your name, address, Social Security number, credit cards, loans, how much money you owe and if you pay your bills on time. All information in the credit report should be about you.

Check your credit report carefully for accounts or other information you do not recognize. You can get one free credit report every year from each credit reporting company (Experian, Equifax and TransUnion). Order online at www.annualcreditreport.com or call 1-877-3228228. Look for mistakes or accounts you do not recognize. This could mean someone has stolen your identity.

Neighborhood Watch

IDENTITY THEFT

Consider subscribing to an identity theft protection service. Several companies offer services to help you in case you become victim to identity theft.

3. Enable Multi-Factor Authentication

Enable multi-factor authentication on every account that offers it, especially banking and emails. This adds an extra level of security, typically requiring a code from an app or a text code in addition to your password.

4. Use strong, unique passwords

Create complex passwords of at least 12 characters using a mix of letters, numbers and symbols. Never reuse the same password for multiple accounts. When shopping online, use strong passwords and only shop on secure websites (have an address that starts with "https").

5. Shred sensitive documents

Never throw away documents containing personal information without shredding them first. This includes bank statements, credit card offers, medical bills, and insurance forms.

6. Protect your Social Security Number, Medicare and Credit Card Information

Leave your Social Security card and Medicare card in a safe place at home. Only share your SSN when absolutely necessary, and ask if another identifier can be used instead. If your Medicare number has been compromised, contact Medicare immediately for a new Medicare number. Photocopy the contents of your wallet. Make copies of credit cards, ID cards and all other personal documents you keep in your wallet. Also, keep records of phone numbers to contact in case you need to close accounts or order replacement items.

7. Secure your physical mail

Collect your mail daily. If you are going out of town, place a hold on your mail at the post office.

8. Limit over-sharing on social media

Avoid posting details that thieves can use to guess your passwords or answer security questions, such as your birthdate, address, or mother's maiden name. Adjust your privacy settings to limit who can see our profile.

9. Use Secure Connections and Software

Ensure your computer spyware is up-to-date. Do not enter personal information and avoid accessing sensitive accounts (like banking) on public computers, such as the library.

Neighborhood Watch

IDENTITY THEFT

10. Recognize and Avoid Phishing Scams

Be skeptical of unsolicited calls, texts, or emails asking for personal information. Do not give your personal information. Be careful with your credit or debit card, and NEVER give out your PIN number. If a company contacts you, do not use the links or phone numbers. Instead, find their official contact information on a trusted website or on the back of your card.

11.. Apply for **IRS Pin**

IRS recommends that you should strongly consider applying for an IRS Identity Protection PIN (IP PIN), especially because it is a free, proactive tool to prevent tax-related identity theft. It is a six-digit number known only to you and the IRS that validates your identity when filing. The fastest way to get one is through the IRS Get an IP PIN tool.

Why You Should Apply (Pros)

- **Prevents Fraud:** It stops thieves from filing a fraudulent tax return using your Social Security number (SSN) or ITIN.
- **Proactive Protection:** Even if you haven't been a victim, opting in protects you, making it much harder for criminals to steal your refund.
- **Easy Filing:** It eliminates issues with e-file rejections if someone else has already tried to claim you or your dependents.

Considerations (Cons)

- **Mandatory Use:** Once you opt into the program, you must use a new IP PIN every year.
- **Loss Risk:** If you lose your PIN, you must retrieve it online or call the IRS.
- **Renewal:** The PIN changes annually and automatically renews.

How to Get an IP PIN

1. **Online (Fastest):** Use the IRS Get an IP PIN tool to register and verify your identity.
2. **Form 15227:** If you cannot verify online and your income is under $79,000 ($158,000 married), you can mail Form 15227.
3. **In-Person:** Visit a Taxpayer Assistance Center.

The IRS will never call, text, or email you to ask for your IP PIN.

<u>If you are a victim of Identity Theft</u>

Notify and file a report with the Police Department**.** This documents the date, time and individual's personal information which helps when dealing with credit monitoring services or bureaus.

The Federal Trade Commission (FTC) website, **IdentityTheft.gov**, is the federal government's one-stop resource for identity theft victims. The site provides streamlined checklists and sample letters to guide you through the recovery process. The FTC cannot resolve individual complaints, but it can provide information about what steps to take. The FTC says that complaints can help them and its law enforcement partners detect patterns of fraud and abuse, which may lead to investigations and stopping unfair business practices.

Important websites:

Federal Trade Commission IdentityTheft.gov

Equifax Equifax.com/personal/credit-report-services 800-685-1111

Experian Experian.com/help 888-EXPERIAN (888-397-3742)

TransUnion TransUnion.com/credit-help 888-909-8872

"KEEP SAFE BY BEING PREPARED

Reviewed and revised. April 2026