NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

Resources

To report identity theft:

IdentityTheft.gov
www.identitytheft.gov/assistant
877-438-4338 | 866-653-4261 (TTY)

To report fraud:

Social Security Administration
www.ssa.gov (Type "fraud" in the search box.)
800-269-0271 | 866-501-2101 (TTY)

Federal Trade Commission (FTC) Consumer Advice
https://consumer.ftc.gov/identity-theft-online-security

USA.gov
www.usa.gov/identity-theft

Identity Theft Resource Center
www.idtheftcenter.org

Credit Bureaus
Equifax: www.equifax.com
Experian: www.experian.com
TransUnion: www.transunion.com

© 2026 QuickSeries Publishing | www.quickseries.com | 29-0115-000-01 | 29-0115-001 | Printed in Canada

My Identity Was Stolen . . . Now What?

Step 1 Call the companies where you know fraud occurred. (You might have to contact these companies again after you have completed an FTC Identity Theft Report.)

- Contact the fraud department. Explain that someone stole your identity.
- Ask them to close or freeze the accounts so no one can add new charges unless you agree.
- Change logins, passwords, and personal identification numbers (PINs) for your accounts.

Step 2 Place a fraud alert and get your credit report.

- Contact one of the three credit bureaus.
- Get your free credit report at: www.annualcreditreport.com or by calling: **877-322-8228**

Step 3 Report the identity theft to the FTC at: www.identitytheft.gov/assistant

QUICKCLICK

If you experienced a scam, fraud, or bad business practice, you can also report it to the FTC at: www.reportfraud.ftc.gov

Filing a Police Report

If you choose to file a report with your local police, bring the following:

- **A copy of your FTC Identity Theft Report**
- **A government-issued photo ID**
- **Proof of address (mortgage statement, utilities bill, etc.)**
- **Any other proof of the theft (IRS notices, bills, etc.)**

Tell the officers your identity has been stolen and you wish to file a report.

Remember to ask for a copy of the police report. You may need this for next steps. This report will prove to businesses that your identity was stolen and provide you with certain rights under Federal law.



Next Steps for Recovery

After reporting the theft, it's time to repair the damage.

- **Close accounts opened under your name.** Call the fraud departments of each business. Ask that they close the account and send you a letter confirming that the fraudulent account isn't yours, you are not liable for it, and it was removed from your credit report.
- **Get fraudulent charges removed.** Tell them which charges are fraudulent and ask for them to be removed.
- **Contact each of the three credit bureaus.** Explain which information is fraudulent and ask that they block that information.
  - Once the information is blocked, it will not show up on your credit report, and companies cannot try to collect debt from you.

QUICKCLICK

To find recovery steps for specific accounts (e.g., utilities, government benefits, loans), go to: www.identitytheft.gov/Steps

Other Possible Steps

Depending on your situation, you may need to take additional steps, including the following:

- **Report a misused Social Security number.**
- **Stop debt collectors from trying to collect debts you don't owe.**
- **Replace government-issued ID.**
- **Clear your name of criminal charges.**

Know Your Rights!

If someone steals your identity, you have the right to:

- File a report with the FTC.
- Place a one-year fraud alert on your credit report.
- Get free copies of your credit report.
- Get fraudulent/inaccurate information blocked from your credit report.
- Get copies of documents related to the theft.
- Stop a debt collector from contacting you.



Protect Yourself from Identity Theft

COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

What Is Identity Theft?

Identity theft is a serious crime – and its damage can be significant and lasting. It happens when someone uses your personal information without your permission.

An identity thief could use your:

- Name and address.
- Credit card and bank account.
- Social Security number.
- Medical insurance account numbers.
- Name and photos on social media.

What can an identity thief do with my personal information?

- Buy things with your credit cards or get new credit cards.
- Open a phone, electricity, or gas account.
- Steal your tax refund.
- Get medical care.
- Use your identity during encounters with law enforcement, other government agencies, etc.
- Create fake accounts online and on social media.

Warning Signs

Identity theft may have already happened if:

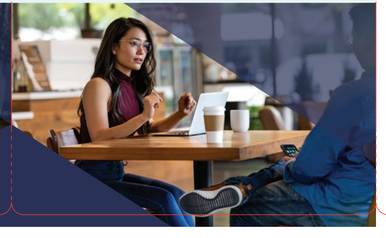
- You see withdrawals from your bank account that you can't explain.
- You don't get your bills or other mail.
- Debt collectors call you about debts that aren't yours.
- You find unfamiliar accounts or charges on your credit report.
- Medical providers bill you for services you didn't use.
- Your health plan rejects your legitimate medical claim because records show you've reached your benefits limit.
- A health plan won't cover you because your medical records show a condition you don't have.
- The Internal Revenue Service (IRS) notifies you that more than one tax return was filed in your name, or that you have income from an employer you don't work for.



How Thieves Get Your Information

Scammers can steal your identity in several ways, including in person, online, through social media, and by phone. Scammers may:

- Steal your wallet/purse to get ID, credit, or bank cards.
- Go through your trash to find bank statements or tax documents.
- Install skimmers at ATMs, cash registers, and fuel pumps to digitally steal bank details.
- Get personal information from your phone when you use public Wi-Fi.
- Use "phishing" to get information from you through fraudulent email, texts, or phone calls.
- Look through your social media accounts to find identifying information in posts or photos. Or they may ask you for personal information in online quizzes and surveys.



Protect Yourself

Here are some steps to take to help protect your personal information and avoid identity theft.

Don't give your personal information to someone who calls, emails, or texts you. It could be a scammer trying to steal your information.

Place a credit freeze and fraud alert on your credit report. With a freeze in place, nobody can open a new credit account. An initial fraud alert tells businesses to check with you before opening a new account in your name.

Keep your financial records, Social Security and Medicare cards, etc., in a safe place. When you decide to get rid of them, shred them before you throw them away.

If you get statements with personal information in the mail, pick up your mail as soon as possible.

Digital Defense Starts Here

Secure Your Home Wi-Fi Network

If malware gets into devices connected to your home network, it can spread to other devices connected to that same network.

Keep Software Up to Date

Update your software programs on your desktop, tablet, and mobile phone as soon as you can when a newer version is released. Turn on automatic updates to automatically update your security software, Internet browser, operating system, and mobile apps.

Use Strong Passwords

If you create your own password, aim for at least 15 characters.

- Use both uppercase and lowercase letters, numbers, and symbols.
- Since a long password can be hard to remember, you may find it easier to use a passphrase (a series of words separated by spaces).
- Use a password manager to generate and store strong passwords.

Multi-Factor Authentication

Multi-Factor Authentication (MFA) offers extra security by requiring two or more credentials to log in to your account.

The credentials you need to log in to your account fall into three categories:

1. Something you **know** (e.g., password, PIN, or answer to a security question)
2. Something you **have** (e.g., one-time passcode sent by text message, email, or an authenticator app)
3. Something you **are** (e.g., scan of your fingerprint, retina, or face)

Where should I use MFA?

- Email
- Social media accounts
- Financial services
- Online stores
- Gaming
- Streaming services

29-0115-001 QS Identity Theft PC8.indd 2
2026-08-07 10:43 AM

COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.