ARAG
Legal Insurance

Identity Theft:
What to Do if Your Identity Is Stolen

Table of Contents

Identity theft is among the top consumer complaints reported to the FTC and other enforcement agencies every year.[1] The damage caused by identity theft can take years – including a lot of time, money and frustration – to repair.

Fortunately, if someone does steal your identity, there are steps you can take to minimize the damage. This guide will help.

What Is Identity Theft?

Identity theft is a serious crime. It happens when someone steals personal information like your name, Social Security number or credit card. Then they use it to commit fraud or other crimes. Identity theft can cost you time and money, destroy your credit and ruin your good name.

In 2022, The Federal Trade Commission received more than 1.1 million online reports of identity theft.[2]

The crime can take a lot of forms. For instance, identity thieves may rent an apartment, sign up for a credit card or open a cell phone account in your name. And you might not find out about it until you look at your credit report or find mystery charges on your credit card statement. Sometimes you won't know until you're contacted by a debt collector.

Some identity theft victims can resolve their problems quickly. But others spend hundreds of dollars and a lot of time fixing the damage.

The impact of identity theft can linger for months or even years. Some victims may lose out on job opportunities. Others may be turned down for loans for college, housing or cars.

And it's all because of negative information on their credit reports. In rare cases, victims have even been arrested for crimes that someone else committed in their name.

Keep Good Records

Think you may have an identity theft issue? Keep track of all phone calls, emails, money spent and time lost from work.

Visit identitytheft.gov for affadavits to file with law enforcement, sample letters to send to creditors and other resources..

Common Types of Identity Theft

Identity theft can touch on many facets of consumers' lives, as reported by multinational consumer credit reporting agency Equifax:

- Child identity theft
- Criminal identity theft
- Employment identity theft
- Estate identity theft
- Financial identity theft
- Medical identity theft
- Synthetic identity theft
- Tax identity theft

What To Do If Your Identity Is Stolen

If you think your personal information has been stolen, take these steps right away:

1. **Put a fraud alert on your credit reports.** This tells creditors to follow certain procedures before they open new accounts in your name or make changes to your existing accounts. You can place a fraud alert on your accounts by contacting one of the three nationwide credit reporting companies.

   - Equifax: 800-525-6285 (equifax.com/personal/credit-report-services/credit-fraud-alerts/)
   - Experian: 888-EXPERIAN (397-3742) (experian.com/fraud/center.html)
   - TransUnion: 800-680-7289 (transunion.com/fraud-alerts)

   As an option, you can also go online to place fraud alerts online with these consumer credit reporting agencies, as well as access educational resources and articles. You do not need to contact all three companies, just one is enough.

2. **Go through your credit report – in detail.** When you place a fraud alert, you're entitled to free copies of your credit reports. Look for inquiries from companies you haven't contacted, accounts you didn't open and debts you can't explain.

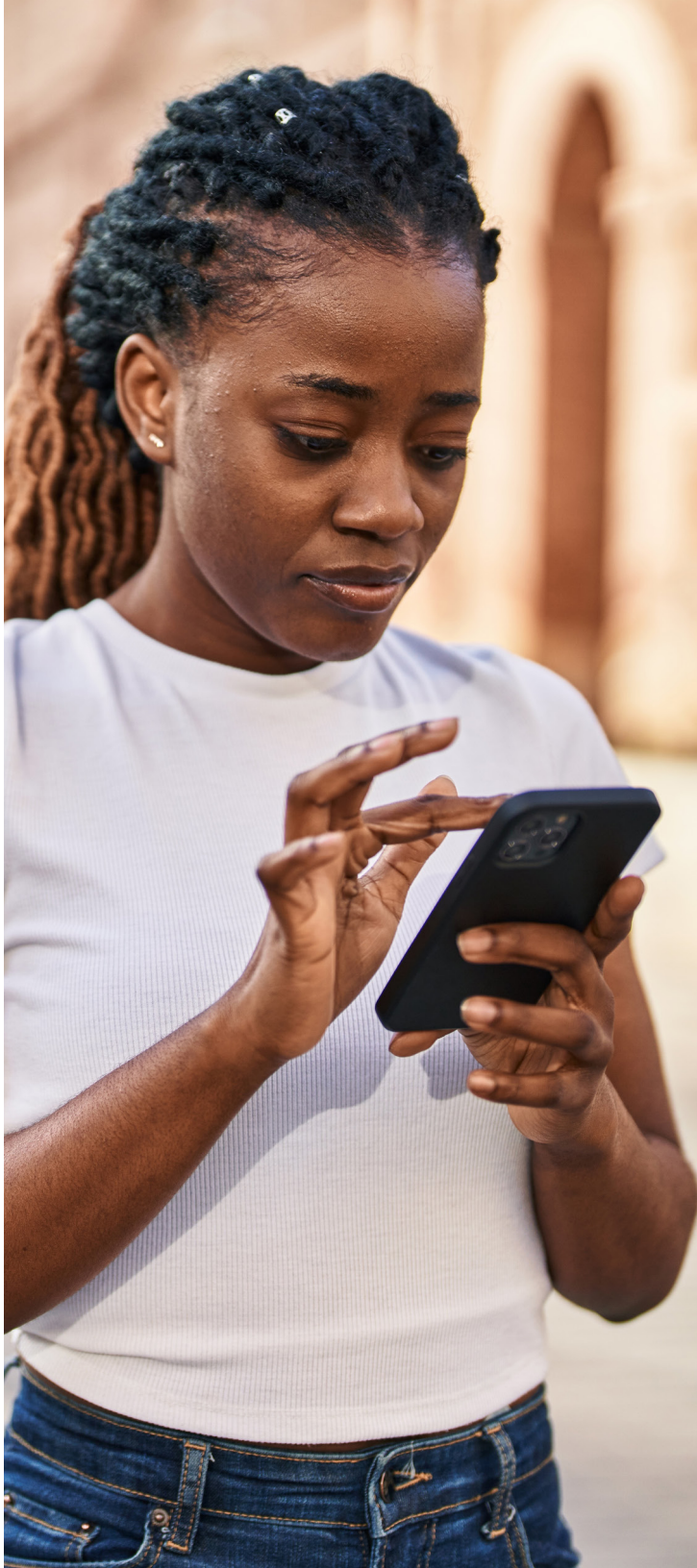
3. **Close any suspect account(s).** If you think an account has been tampered with or opened without your permission, close it. And keep these tips in mind:

   - Contact the security or fraud department of each company. Follow up in writing, and include copies of supporting documents. Send your letters by certified mail – return receipt requested – so you can document what the company received and when.
   - When you open new accounts, use new personal identification numbers (PINs) and passwords. Avoid using information that's easy to steal – like your mother's maiden name, your birth date, the last four digits of your Social Security number, part of your phone number or a series of consecutive numbers. Use the Identity Theft Affidavit at identitytheft.gov to support your written statement.
   - Ask the company holding your account to verify in writing that the disputed account has been closed and the fraudulent debts removed.
   - Keep copies of all documents and records of your conversations about the theft.

4. **File a complaint with the Federal Trade Commission (FTC).** You can use their online complaint form at reportfraud.ftc.gov. Or call the FTC's **Identity Theft Hotline 1-877-ID-THEFT (438-4338)**; **TTY: 1-866-653-4261**. You may want to provide a printed copy of your complaint form to the police to incorporate into their police report.

5. **File a police report.** File a report with law enforcement officials to help provide proof of the crime to creditors.

6. **Monitor your credit report quarterly.** Once the problem is resolved, you can scale back to annual reviews.



What To Do If...

Not sure what to do in specific situations involving identity theft? Use these guidelines:

Debt collectors are trying to collect charges you didn't make.

- ✔ Request in writing that the collection agency stop contacting you.
- ✔ Send your letter by certified mail – and request a return receipt.

Legally, a debt collector can't contact you if you send a letter and supporting documentation saying that you don't owe the money within 30 days of getting written notice from them. Keep in mind that the letter may stop collection activity, but the debt itself may show up on your credit report.

You have fraudulent information in your credit report.

- ✔ Send the credit bureaus a copy of an identity theft report and a letter telling them what information is fraudulent. Tell them that you didn't make or authorize the transactions.
- ✔ Provide proof of your identity – like your Social Security number, name and address.

The credit bureau has four business days to block the information after accepting your identity theft report. It must tell the information provider that it has blocked the information.

Your passport is stolen.

Contact the U.S. Department of State (USDS) – Passport Services. You'll be asked to complete Form DS- 64, Statement Regarding a Lost or Stolen Passport.

Your mail has been stolen and used to get new credit cards or to steal your personal information.

Report the incident to your local postal inspector by phone (1-877-876-2455) or at uspis.gov

You have fraudulent charges on your credit cards.

- Write to the creditor at the address given for "billing inquiries" (not the address for sending your payments). Include your name, address, account number and a description of the billing error, including the amount and date of the error.
- Send your letter by certified mail, and request a return receipt. Include copies (not originals) of your police report or other documents that support your position. Keep a copy of your letter.

The creditor has to acknowledge your complaint in writing within 30 days after receiving it, unless the problem has been resolved. The creditor must resolve the dispute within two billing cycles (but not more than 90 days) after receiving your letter.

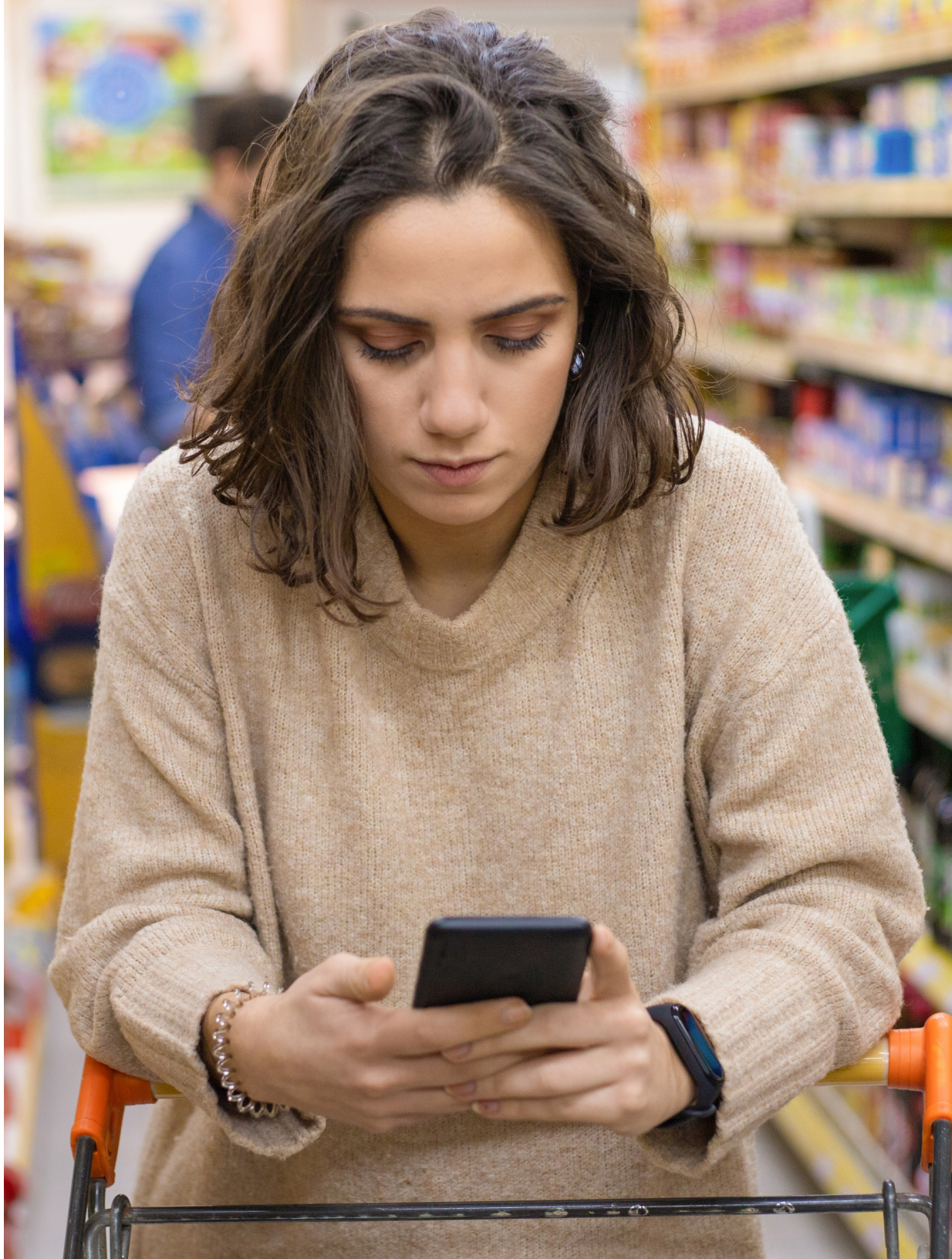
Your checks are stolen or misused.

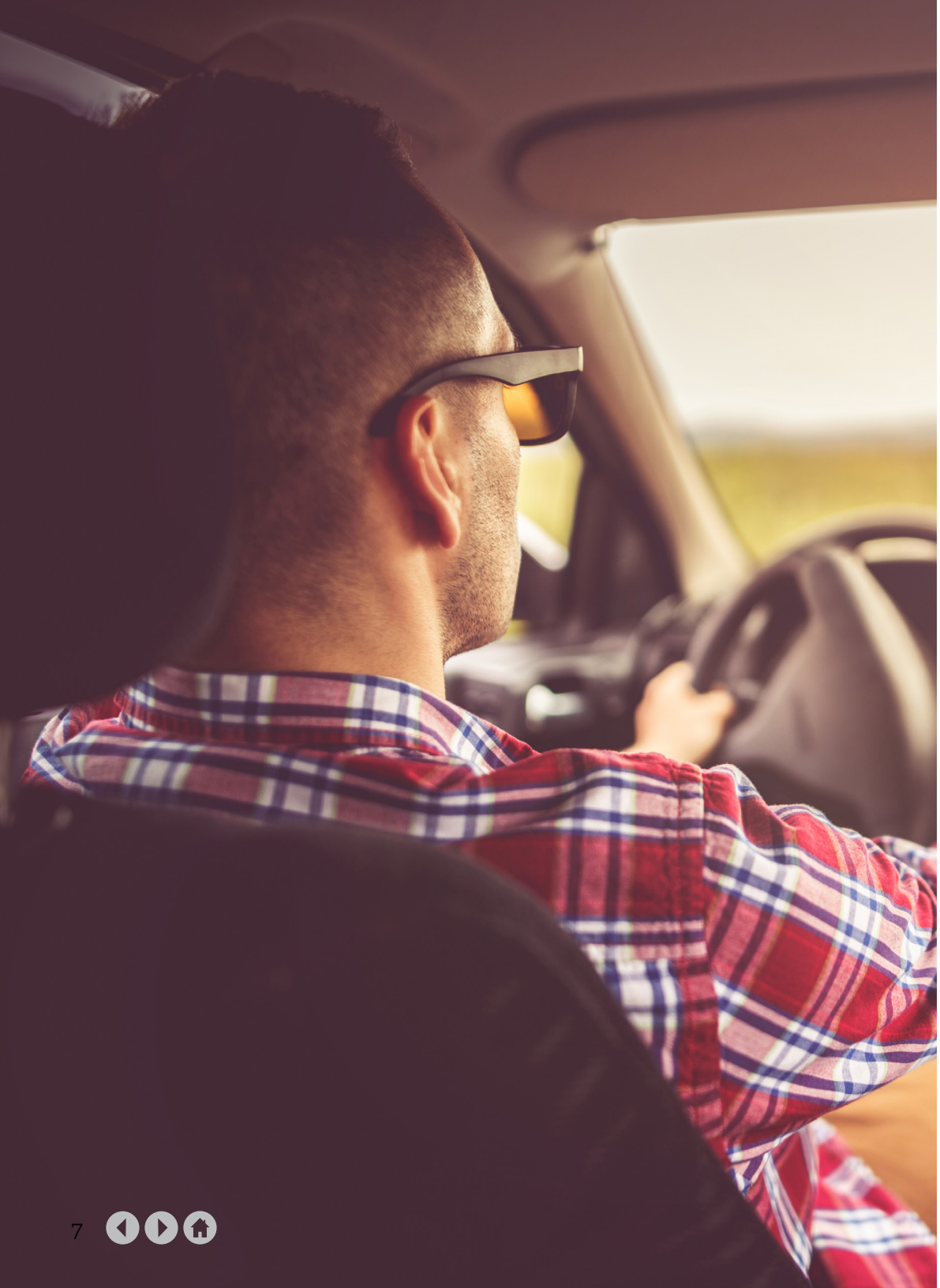
- Stop payment.
- Close the account.
- Ask your bank to notify Chex Systems or the check verification service it uses. That way retailers can be notified not to accept these checks.

If someone misuses your checks, most states hold the bank responsible for losses. But if you don't let the bank know about the situation promptly, you may be on the hook for most (or all) of the losses.

Your Social Security number is being misused.

Contact the Social Security Administration to request a replacement card or obtain a new Social Security number. You should also file a police report.





Someone uses your identity to commit tax fraud.

Call the Identity Protection Specialized Unit at 800-908-4490, ext. 245 or visit irs.gov

Your debit card is lost or stolen.

- Call the financial institution and follow up in writing by certified letter (request a return receipt). Keep a copy for your records.
- The amount you're responsible for depends on how quickly you report the loss.
  - If you report the loss of the debit card before someone uses it, you are not responsible for any unauthorized transactions.
  - If you report it within two business days, your loss is capped at $50.
  - If you report it after two business days but less than 60 calendar days after your statement containing the unauthorized transactions is sent to you, you could lose up to $500.
  - If you report it more than 60 calendar days after your bank statement containing the unauthorized transfer is sent to you, you could lose all money that was taken.

After getting your notification, the institution generally has 10 business days to look into it. They have to share results within three business days after completing their investigation. And they must correct an error within one business day after determining that it happened.

If the institution needs more time, they can take up to 45 days to complete the investigation. In the meantime, they have to return the money in dispute to your account. At the end of the investigation, if no fraudulent charges were found, the institution must notify you in writing before taking back any money that was returned to your account during the investigation.

Someone uses your identity to get a driver's license.

Contact your Department of Motor Vehicles. If your state uses your Social Security number as your driver's license number, ask to substitute another number.

Someone uses your identity to commit a civil crime.

- Contact the Federal Bureau of Investigation (FBI).
- Contact the police or sheriff's department that arrested the person using your identity or the court agency that issued the arrest warrant.
- Think about hiring an attorney to help you clear your name.
- File an impersonation report and have your identity confirmed. The police will compare your fingerprints, photos and identifying documents – like your driver's license and passport – to the imposter's.
- The law enforcement agency should recall warrants and issue a clearance letter or certificate of release (if you were arrested or booked). Keep the document with you at all times in case you're wrongly arrested.
- Ask the law enforcement agency to issue an amended complaint by filing the record of your innocence with the district attorney's office and/or the court where the crime took place.
- If your name is in the criminal database, it's tough to remove it completely. Ask that the "key name" or "primary name" be changed from your name to the imposter's name, with your name noted only as an alias.
- Determine which state laws will help you clear your name in the state records. If your state has no formal procedure for clearing your record, contact the District Attorney's office in the county where your case was originally prosecuted. Ask for the court records needed to clear your name.

Someone uses your identity to get health care benefits or access your records.

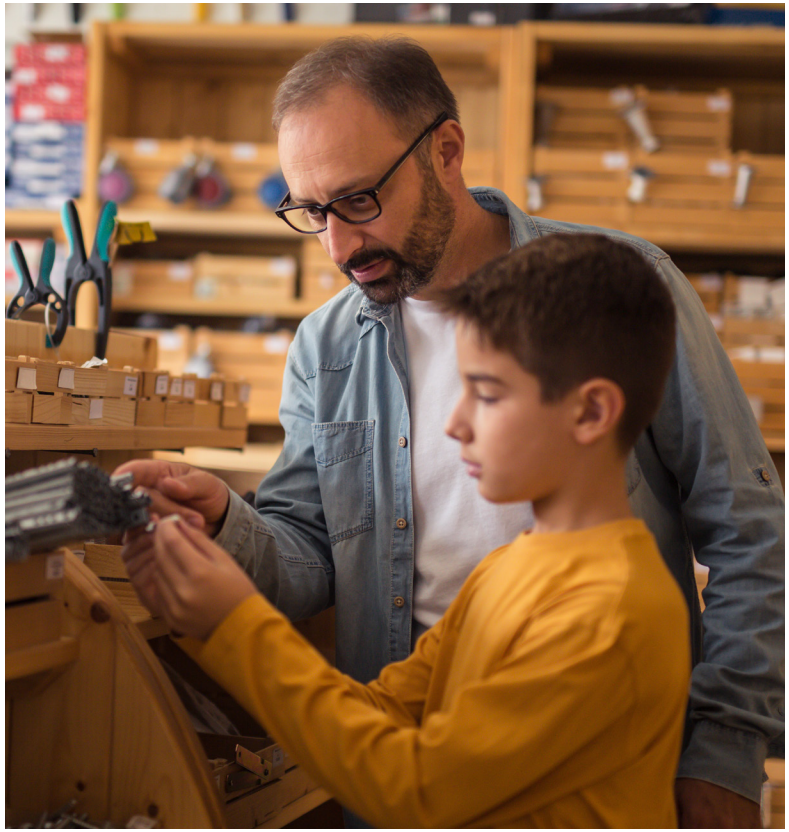
- Look at your records with your health care provider and determine what's accurate.
- Notify the Office for Civil Rights.
- If MediCare fraud is suspected, visit oig.hhs.gov/fraud/hotline or call 800-447-8477 (1-800-HHS-TIPS).

Someone uses your identity to get a student loan.

- Ask the school or program that opened the student loan to close it.
- Report the fraudulent loan to the U.S. Department of Education.

Someone uses your identity to file bankruptcy.

- Write to the U.S. Trustee in the region where the bankruptcy is filed. Your letter should describe the situation and provide proof of your identity. If appropriate, the U.S. Trustee will make a criminal referral to law enforcement authorities if you can substantiate your claim.
- Consider filing a complaint with the U.S. Attorney or the FBI.
- You may need to hire an attorney to work with the bankruptcy court and help demonstrate the filing is fraudulent.



Someone uses your identity to open bank accounts.

- Contact each of the banks where account inquiries were made. This will help make sure that any fraudulently opened accounts are closed.
- Request a free copy of your consumer report by contacting Chex Systems, Inc. If you find inaccurate information, follow the procedures under "Correcting Fraudulent Information in Credit Reports" to dispute it.

What should I do if I've done everything advised and I'm still having problems?
Sometimes you can do everything right and still spend years dealing with problems related to identity theft. The good news is that most people can get their cases resolved eventually. You just need to be persistent, assertive and organized.

Remember:

- Don't put off contacting companies to address the problems.
- Don't be afraid to go up the chain of command or make complaints, if necessary.
- Keep organized and detailed files.
- If you haven't filed a complaint with the FTC or updated it, you should do it. Make sure you give details of the problems you're having.

If your problems are due to a person or organization not fulfilling legal obligations, you may want to contact an attorney who specializes in that kind of violation.

Someone tampers with your securities, investments or brokerage accounts.

- Contact your broker or financial account manager.
- File a detailed complaint with the SEC.

Take Control with ARAG

If you have questions or aren't sure where to turn, ARAG can help. Visit ARAGlegal.com to learn more about how ARAG legal coverage gives you an affordable way to manage legal matters.

[1]"Consumer Sentinel Network, Databook 2022." Federal Trade Commission, February 2023. https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf
[2]"New FTC Data Show Consumers Reported Losing Nearly $8.8 Billion to Scams in 2022." https://www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022