ARAG

Legal Insurance

# An Overview On
# *Identity Theft*

Identity theft is a serious crime. It occurs when personal information, such as your name, Social Security number or credit card, is used without your knowledge to commit fraud or other crimes. Identity theft can cost you time and money, destroy your credit and ruin your good name. Of the 6.5 million reports made to the Federal Trade Commission in 2024, identity theft was the second most common with over 1.1 million reports.[1]

Identity thieves may rent an apartment, obtain a credit card or establish a telephone account in your name. You may not find out about the theft until you review your credit report or a credit card statement and notice charges you didn't make – or until you're contacted by a debt collector.

While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many hours repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

### *New Partners in Crime:* Identity Theft and Artificial Intelligence

A new era of identity theft is on the horizon, as cybercriminals have taken up newly forged artificial intelligence (AI) voice cloning tools to create a new breed of scam. With a small sample of audio, they can clone the voice of nearly anyone and send bogus messages by voicemail or voice messaging texts.

# *Table of Contents*


**How Do I Prevent Identity Theft?** *3*

**Tips to Keep Your Private Information Secure** *4*

**Heads Up! Child, Senior Identity Theft On the Rise** *6*

**What To Do If Your Identity Is Stolen** *7*

**What To Do If...** *8*

**Other Resources** *12*


# How Do I Prevent Identity Theft?

To minimize your risk of becoming a victim of identity theft, simply remember SCAM.

*S*

**Be STINGY when it comes to giving out your personal information, unless you trust the person asking.**

Adopt a "need to know" approach to your personal information. For example, limit the information you provide online or over the phone. Among the most important elements of your identity to protect? Your Social Security number, date of birth or cell phone number.

If someone calls to offer you a credit card, a prize or other valuable item but asks for personal data such as your Social Security number, credit card number or mother's maiden name, ask the person to send you a written application form. If they won't do that, say you're not interested and hang up. If you do receive an application, review it carefully to make sure it's going to a company or financial institution that's reputable. Check to see what businesses have received complaints with the Better Business Bureau.

*C*

**CHECK your financial information regularly.**

Monthly statements for bank and credit card accounts should list transactions for the most recent reporting period. Always check these statements carefully. This is the quickest way to find out if unauthorized debits or credits are being made to your accounts.

If you're not receiving monthly statements for accounts you use, contact your financial institution or credit card company. If the statements are being mailed to another address that you didn't provide, let them know right away that someone may be improperly using your accounts.

If someone is making withdrawals, charges or opening accounts in your name, contact your financial institution or credit card company immediately to report these transactions and to ask for the bank to take action.

*A*

**ASK for a copy of your credit report routinely.**

The Federal Trade Commission (FTC) encourages consumers to review their credit reports every year. Clear up misinformation as soon as possible to keep from jeopardizing your credit rating or stalling your application for any credit purchase.

You can get one free credit report a year from each of the three major credit bureaus by visiting AnnualCreditReport.com. This is a free site that will not ask for your credit card number or try to sell you additional services.

Your credit report should list all accounts under your name and will provide evidence if someone has opened or used any accounts wrongfully.

*M*

**MAINTAIN careful records of your banking and financial accounts.**

Retain monthly statements and checks for at least one year. This way, if you need to dispute any transaction, especially one that claims to bear your signature, your personal records will be more immediately accessible and useful to the institutions.

# Tips to Keep Your Private Information Secure

If you're in over your head with debt, the worst thing you can do is ignore the problem, because it will only get worse. Follow these steps to help get back on track:

**Keep your Social Security card secure.**

- Never carry your Social Security card in your wallet.
- Be cautious of anyone asking for your Social Security number. If they refuse to complete a transaction without it, consider taking your business elsewhere.

**Keep your credit cards safe.**

- Make sure new cards arrive in a timely manner and sign them as soon as you receive them.
- Keep a record of your account numbers, expiration dates and contact information of each company in a secure place.
- Carry only cards you think you'll need, and consider canceling cards that you haven't used in the past six months.
- Never lend your card to anyone.
- Shred old cards when you dispose of them.

**Review credit card statements, phone and utility bills monthly.**

- Consider switching to online accounts to receive statements, invoices, etc., to reduce paper, streamline your viewing process and limit the amount of physical statements, bills, etc. that are saved (and at risk of being stolen).
- Call the company if you don't recognize a charge or phone call.

**Keep your mail safe.**

- Install a locking mailbox or a mail slot that goes directly into your house.
- Send your mail, especially payments, directly from the post office (don't put it in the mailbox for the postal carrier to pick up).
- If your bank allows, pick up your new checks from the bank instead of having them sent to your home.

**Shred or tear up personal information when you throw it away.**

- Always take your credit card receipts and never throw them away in public.
- Tear up or shred any offers for pre-approved credit cards you don't intend to use and beware of offers from companies you don't recognize.

**Don't give personal information over the phone unless necessary.**

- Never give personal information unless you made the phone call.
- If someone calls and says they are calling from your bank or credit company, ask for a number to return the call. Make sure it's an official number before calling back.

**Limit the information you put on checks.**

- Don't preprint your Social Security number, phone number or your driver's license number on your checks.
- Don't pre-print your full name on checks. Use only your initials and last name. If someone takes your checks, they will not know if you sign your checks with just your initials or your full name, but your bank will know. If you have one, list a P.O. box on your checks instead of your home address.

## Guard Your Online Information and Identity

**Change up your passwords and PINs.**

- Ensure that you avoid using the same password or PIN (Personal Identification Number) – or variations of it – which makes it that much easier for a thief to "crack the code" across multiple devices and accounts.
- Change your passwords and PINs regularly.
- Don't use common codes like birthdays or the name of your spouse, child or pet. Memorize passwords and your PIN and shred any piece of paper on which they are written.

**Monitor the information you provide online.**

- Don't put personal information on a computer home page or personal computer profile.
- Be careful about the type of information you put on social media. For example, be wary of online questionnaires or quizzes that ask for intriguing facts or personal information about you.
- If you find your personal information posted on the internet, demand that it be removed.
- Avoid using public Wi-Fi networks when possible, as it may expose your personal and financial information to hackers and scammers.
- Update your virus protection software routinely. Use a firewall program and a secure browser.
- Don't reply to pop-up or spam messages on your computer.
- Be cautious about opening attachments and downloads.
- Delete personal information when you dispose of a computer. Use a "wipe" utility program that overwrites the entire hard drive and makes the files unrecoverable.

# Heads Up! Child, Senior Identity Theft On the Rise

Child identity theft usually involves thieves who are mainly interested in stealing a child's Social Security number, which can then be:

- Sold to the highest bidder.
- Used to apply for things like government benefits, open bank and credit card accounts, apply for a loan, receive medical treatment or rent a place to live.
- Crafted to create a new identity.

A child is seen as a desirable target for identity thieves mainly because minors are not old enough to apply for a credit card, a loan, etc., so they have a "clean slate" of credit history thieves can take advantage of.

Conversely, criminals see the elderly as perfect targets for different reasons: in general they are trusting, not quite as technologically savvy and often have large savings or retirement accounts. They can often fall prey to phone and online scams where urgent or fake requests for money or information are demanded. Or they can be victims of insurance fraud, (whether it be for medical, auto, home, etc.) when trying to manage bills, medical records, EOBs (Explanation of Benefits), submitting claims, etc.

Plus, as senior citizens grow older, many of them need help from caregivers (either at home or at assisted-living facilities/nursing homes) who have access to financial and medical records that include sensitive personal information.

# 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.

### 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.

### Someone tampers with your securities, investments or brokerage accounts.

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

### 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.

# Other Resources

**Department of Justice**
justice.gov

**Federal Trade Commission**
identitytheft.gov

**Equifax Credit Information Services Consumer Fraud Division**
P.O. Box 740241
Atlanta, GA 30374-0241
888-766-0008
equifax.com/CreditReportAssistance/

**Experian's National Consumer Assistance**
P.O. Box 2002
Allen, TX 75013
888-397-3742
experian.com/fraud/center.html

**TransUnion's Fraud Victim Assistance Department**
P.O. Box 2000
Chester, PA 19022-2000 8
800-680-7289
fvad@transunion.com
transunion.com/fraud

[1]Federal Trade Commission, Consumer Sentinel Network, Databook 2022, 2024, Released March 2025. https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf

## Be Prepared When *Legal Happens*

Visit **ARAGlegal.com** to explore how legal coverage can help with debt, budgeting and more, empowering you to take control of your financial future.

### Already a member?

Log into **ARAGlegal.com/account** to view the Learning Center, confirm coverage, start a case, read attorney reviews and much more.


Legal Insurance



100020