AMG National Trust

A Better Way To Wealth

FACT FILE

ID THEFT & FRAUD

Keep Your Guard Up

You could be the victim of a mugging and not even know it.

Years ago, safety was probably uppermost in our minds when walking along the street. These days, we stroll the information superhighway and casually share our personal information across online shopping and social media. We give out credit card numbers while on cellphones or type in a PIN at an ATM without concealing them from prying ears and eyes. We click on random emails or links in texts without being certain of the source. As a result, identity theft and fraud "muggings" are increasing annually, but only about 1 in every 700 of the culprits are ever caught and prosecuted. When theft or fraud happens, you may not realize it until long after the incident. The good news is that there are ways to protect yourself.

Costs to Consumers

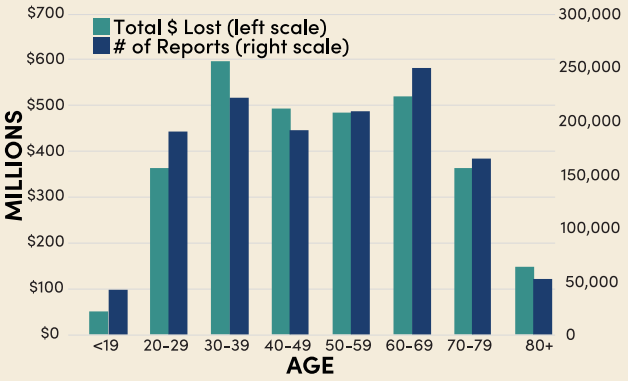
Identity theft begins when someone takes personally identifiable information, such as your name, Social Security number (SSN), date of birth, your mother's maiden name, or your address, to use, without your knowledge or permission, for their personal financial gain.

How common and how costly are identity theft and fraud in the U.S.? The Federal Trade Commission received more than 5.7 million reports of overall fraud in 2021, an increase of about 1 million from 2020. Individuals reported losing more than $5.8 billion, with a median loss of $500.

Individuals are not the only target. Businesses lost an estimated $56 billion in 2020 through data breaches or ransomware attacks, according to one study. Equally alarming is that a data breach at a single company can result in the theft of thousands or millions of identities in one fell swoop.

Consider adopting a zero-trust contact policy—when a stranger initiates unexpected contact, keep your guard up.

Reported Frauds and Losses by Age



Source: Federal Trade Commission, Consumer Sentinel Network Data Book 2021

Fast Facts

- Government documents and benefits fraud topped the list of U.S. identity theft types in 2021, as criminals used stolen or fake identities to illegally obtain pandemic benefits. The next leading source of U.S. identity theft was credit card fraud.
- Men and women have a nearly equal likelihood of falling victim, according to the U.S. Department of Justice.
- States with the highest per capita rates of reported fraud in 2021 were Georgia, Maryland, and Delaware. For reported identity theft, Rhode Island, Kansas, and Illinois were at the top.

Types of Fraud: These May Sound Familiar

Knowing how thieves work—the circumstances that create identity theft/fraud risks—should help you defend against them. The schemes can be low tech or high tech. But low-tech activities such as these—and note there are many more—have remained a staple.

- **Contractor fraud.** A typical scenario involves an uninvited door-to-door solicitation from a contractor claiming to have a "special price" on roofing, siding, windows, asphalt, or other services, often after severe weather, such as hailstorms, high winds, or flooding. They may say they have done work for neighboring houses and have extra materials that they can offer at a discounted price. Such tactics are typically not criminal, but your defenses should probably go up if they insist that you have damage that must be repaired right away or if they require a substantial payment in advance.

  A general rule of thumb for hiring a contractor is to get three written bids, but do not necessarily choose the lowest one. Consider asking the bidders to submit a written contract that lists materials, costs, and the completion date. You may also want to require your contractor to obtain mechanic's lien waivers from all suppliers and subcontractors. Another option is to check out the contractors with the Better Business Bureau (BBB) or your state's regulatory agencies. Websites devoted to customer reviews and ratings can be helpful as well.

- **Caregiver fraud.** Caregivers in the home are often a vital resource for older individuals, but that also opens the door to potential exploitation. Older people who are coping with loneliness or confusion can be particularly susceptible to financial, physical or emotional abuse. A caregiver might try to isolate the patient, who then comes to rely solely on the caregiver.

  Consider seeking a caregiver through a bonded and insured homecare agency and consider asking about credentials for managing specific health needs.

  Warning signs of financial abuse by a caregiver can include: odd bank account activity; items in the home that go missing; changes to wills, trusts or powers of attorney; giving away money; or signing over the home.

  To shield your loved one, a good idea may be to create an inventory of all valuables in the house. If the caregiver buys groceries or runs errands, you could consider giving them a prepaid debit card to pay for those. You may also want to make unannounced visits to the home or ask a friend of your loved one to stop by. Consider installing a doorbell video camera to know when the caregiver comes and goes. Other ideas include getting to know your loved one's banker and asking about the bank's "age-friendly services" for older clients, such as alerts for specific account activity and opportunities to name trusted third parties to view or receive information on their accounts.

  Banks are on the front line for warning signs of older clients being victimized, such as when they withdraw more money than usual, visit a branch more frequently or are accompanied by a family member or caregiver when none of these behaviors were the case previously. Since 2016, when the U.S. Consumer Financial Protection Bureau offered uniform guidance to financial institutions on protecting older customers—the first time a federal regulator had provided such extensive suggestions for best practices—industry groups, lawmakers and state regulators have moved to implement some of the recommendations.

- **Medicare scam.** In 2018, Medicare started issuing new cards to beneficiaries intending to improve identity theft protection. However, this gave rise to new scam opportunities that targeted seniors, including scammers asking members to update their information or pay a fee to receive new cards. Medicare completed this rollout in 2019, so these kinds of requests from the agency are no longer valid. You should call Medicare at 1-800-MEDICARE (1-800-633-4227) if anyone contacts you for personal information or money. If a Medicare representative needs to talk to you, you should first receive an official letter from the Social Security Administration to arrange a telephone interview.

- **Grandparent scam.** Perhaps you'll receive a late-night call from someone posing as your grandchild. In this example, the person explains, in a frantic-sounding voice, that he or she is in trouble, maybe claiming there's been an accident, an arrest, or a robbery. To increase the drama and urgency, the caller might claim to be hospitalized or stuck in a foreign country; to make the impersonation more convincing, he or she may throw in a few family particulars, gleaned from the actual grandchild's social media activity. The "grandchild" implores you to wire money immediately, adding an anxious plea: "Don't tell Mom and Dad!"

  The smart move is to hang up and call the grandchild or other family member in question, on a known number, to make sure they're safe. With luck, they'll answer, and you'll know the supposed

emergency call is a scam. You should then notify your local authorities.

- **This is the IRS calling.** Have you been told about taxes you owe, missing tax forms, or liens and levies that require immediate payment to resolve? Or has an "agent" called after a hurricane, tornado, or flood to help you file casualty loss claims and get tax refunds? Yet another angle involves COVID-related scams that accuse you of Paycheck Protection Program (PPP) fraud or claim you're due extra or overdue stimulus payments or unemployment checks.

  The IRS should never initiate contact with any taxpayer by phone, text message, email, or social media channels to request personal or financial information. If unsure, log into your IRS account to see the status of your tax returns and/or benefits. The IRS website is www.irs.gov. Taxpayers should not be misled by any site claiming to be the IRS whose address ends in ".com," ".net," ".org," or another domain suffix.

- **Fraudulent filing.** Filing forged tax returns and attempting to get a fraudulent refund early in the filing season is also common. Taxpayers may be unaware they have been wronged until they file their tax return later in the season, only to discover a return has already been filed using their SSN. Although no liability is assigned to the taxpayer, their refund will likely be delayed for months.

  The IRS encourages taxpayers to file returns early and is on alert for returns that hint of identity theft but contain a real taxpayer's name and/or SSN. When a suspicious return such as this is received, the IRS should send the taxpayer a 5071C letter, which asks the taxpayer to verify his/her identity. The identity verification service website, www.idverify.irs.gov, was created as a fast, easy way to complete this task.

  For added protection, tax filers can request an Identity Protection PIN (IP PIN) from the IRS. The PIN is a six-digit number known only to you and the IRS. If you are a confirmed victim of tax-related identity theft and your tax account issues have been resolved, the IRS should mail you a CP01A Notice with a new IP PIN each year. You can also request one at www.irs.gov/IPPIN. Filers cannot opt out once the IP PIN is used.

- **Utility company scams.** In this scenario, you may receive a "final notice" via email or text that demands payment to avoid a shutdown in service. Or the notice might promise refunds via direct deposit or check, so long as you tell them where to send it. Be aware that you'll probably receive multiple advance notices if your account really is past due. Consider calling your utility company directly to confirm the past due amount and how you should pay.

- **Prize/gift card grift.** What happens if you receive a text or email from a store or organization saying you've won a prize or gift card, but they say more contact information is needed before they can send the gift to you? They may then provide a link to a series of questions about your finances or other sensitive details, the answers to which may allow the thief to steal your identity and sell your data to others. Before anything else, consider asking for a callback number, and then look up the organization to contact them and verify the gift.

- **Dumpster diving.** Imagine someone goes through your garbage to obtain personally identifiable information from items found in the trash, such as credit card bills, utility bills, medical insurance, and bank statements.

  To protect yourself, it's advisable to shred everything with a cross-cut paper shredder before disposing of it. Another protection method is to go paperless by receiving statements and making your payments online. It's also a good idea to keep track of your credit report and report any discrepancies to your credit card company and credit bureaus.

- **Mail theft.** Many of us have non-locking mailboxes that anyone can access. Bad actors may steal mail from your box or submit a change of address form to the post office to re-route mail without your knowledge. If you suspect that someone has been taking mail from your box, you should contact the post office immediately. To be proactive, consider using a locking mailbox if possible or rent a box at the post office.

  The post office also offers Informed Delivery service, where you can receive an email with grayscale images of the exterior, address side of up to 10 pieces of incoming letter-sized mail that will be arriving soon. Package tracking notifications also are available. You can set up the service at www.usps.com.

- **Social engineering.** In this instance, someone will try to deceive you into divulging sensitive information through the telephone, computer or in person. To do so, they will probably incorporate some information that leads you to believe they are legitimate.

You should probably avoid divulging any personal information to someone you don't know, and you should be careful about what you share online and with whom you share it. When in doubt, ask for a contact number and verify it with the company they say they represent.

- **Shoulder surfing.** Is someone standing a little too close when you're entering a PIN at an ATM or store checkout line? Don't be afraid to ask them to move back. You also could instead use cash for your transaction or use a prepaid credit card.
- **Stealing personal items**. Keep a purse shut tight and hold it close to your body. If you carry a wallet, you may want to button the back pocket where you stash it or put it in a front pocket. Also, consider how much you carry with you; security experts recommend leaving your Social Security card at home, along with credit cards you use infrequently. You should also consider removing old deposit slips, blank checks, and any information that carries your login and password information.
- **Child identity fraud.** Children are at risk because their SSNs are not associated with a credit history, which typically makes it easier to create fraudulent IDs from their information. This theft might not be discovered until the child is old enough to apply for a job, student loan, or apartment. Red flags may include receiving letters in the child's name for debt collection, preapproved credit offers, and tax notices and traffic tickets; or receiving IRS letters saying your child is already claimed as a dependent on someone else's tax return.
- **Home title theft.** Using a stolen identity, a thief may be able to forge a deed to pretend they own a property or take the cash from a home equity loan or refinance. Foreclosure may occur if the loan goes into default. Or they might target a vacant home and sell it without the owner's knowledge. As a shield, owners should consider carrying title insurance and staying on top of bills for their properties.

What's Already on the Internet can be Used Against You

Mobile phones, tablets, computers and other devices, and the personal information we've loaded into them, make financial and other transactions far simpler, but you should also take stock of your security measures. Three steps are recommended: 1) install an antivirus and keep it updated; 2) don't ignore those annoying pop-ups prompting you to restart your device for a software update; and 3) use a different password/PIN for each login, then write them down and store them safely for later reference. Other protection methods worth considering include turning on two-factor authentication wherever possible; locking your screen when done viewing it; using a VPN; and avoiding public Wi-Fi.

At a store, have you seen someone hold a phone over a point-of-sale machine to make a purchase? They're probably using a digital wallet, which typically encrypts and tokenizes data so that it's useless to criminals if stolen. (Tokenization involves moving sensitive data to a secure location and replacing it with a "token," or placeholder, until the sensitive data is needed and retrieved.) Digital wallets are available from many well-known tech companies; they may charge transaction fees.

Digital Wallets

A digital wallet can be used to store information about your payment methods, coupons, gift cards, and more in one central location. It can be a convenient, secure way to organize all your information, so you don't have to carry a wallet full of plastic cards.

One downside is that not all providers offer two-factor authentication (i.e., entering a unique code from an app after logging in), which is a recommended security feature. Another concern is that because mobile phones and wearables use wireless networks, hackers could potentially access that data. Finally, there is the risk you may lose your device, along with all the data on it.

How to Make a Payment Through a Digital Wallet App

1. User downloads a digital wallet app
2. Bank account or card information is linked to the app
3. Account information is encrypted
4. Wallet becomes available after user authorization
5. User holds their smartphone close to the contactless payment terminal to pay

Source: TechTarget

Despite our best efforts, some cybercriminals will still get through. Here are some examples of methods they may use:

- **Phishing.** Phishing scams—or fake emails that appear to be from a well-known source—remain one of the most common identity theft scams. One trending cybercrime relates to fake delivery services from companies you've done business with. Impersonators will relay a problem with your order and ask you to click a link to correct the issue. The link then takes you to a company website that mirrors the real one, and you'll be asked to input account information that would go directly to the scammers.

  One recommendation is to be suspicious of any communication with urgent requests for personal financial information. You should avoid clicking on a link to unsolicited "update your password" emails without verifying the source (such as hovering over the email address in the "from" line). It's also advisable to avoid opening attachments on unexpected emails and to install robust antivirus and anti-malware software.

- **Email/text message come-ons.** These come-ons can be an alert, or what seems like a reply to one of your messages, encouraging you to call a 900 or other toll-based number, or open a mysterious web page. You're then often directed to a phishing website under the pretense of a job offer or quick cash, or the threat of legal action over an unpaid bill. Ultimately, the scammer usually aims to trick you into giving up sensitive or personal information, such as a banking site password.

- **Online shopping.** By 2025, an estimated 291.2 million Americans will be shopping online, per Statista. Every shopper online has typically already released to the Internet a treasure trove of personal information—phone numbers, home addresses, and credit cards. To a cybercriminal, that information is like striking gold. So, before you shop, you may want to look at the website URL at the top of the page. If it begins with "https" instead of "http," or includes an image of a lock, it generally is secure for your use. Do you have antivirus software? If so, it should throw up a warning when you come across an unsecured site.

  Cybercriminals will also create websites that mimic actual sites and try to trick shoppers into purchasing something off the fake site. These can pop up in Internet searches or as a link in an email or text message. The company name will often look very similar to what you may expect, but with a subtle difference, for example, www.fakec**o**mpany.com versus www.fakec**O**mpany.com.

  Other details to look for: A legitimate business will be more likely to list a physical address, phone number, or return policy on their website.

- **Credit/debit card theft.** First, let's go over ways to protect yourself. You can sign up for free credit-monitoring services that alert you to activity on your credit report. You can freeze your credit, meaning no new accounts can be opened in your name (and it's typically easy to unfreeze your credit when needed). You can set up multi-factor authentication, which adds a step when you log into your accounts, such as retrieving a code via text or email. Also, you can write CID on the signature panel instead of your signature on the back of your card. CID stands for "SEE ID" and requires merchants to request to see other forms of identification to verify the user of the card.

  The following frauds can be used against both credit and debit cards:

  Card not present (CNP) fraud happens when a criminal uses the numbers of your credit card to make purchases online, by mail, or over the phone. In these cases, they do not have to present the physical card to a merchant. Merchants can work to prevent this type of fraud by using biometrics for identification or verifying an identity with information like a mailing address.

  Counterfeit and skimming fraud occurs when a device, most commonly a credit card skimmer, is attached to either an ATM or a merchant's terminal to steal the details of your credit card from its magnetic stripe. Skimming can also occur when someone brushes past you with a credit card skimmer. Details obtained via skimming can then be used to create a counterfeit card.

  Lost or stolen card fraud is fairly self-explanatory—if your card has been stolen, whomever has it can use it till the card is canceled, suspended or it has reached the credit limit. You can avoid the worst of the damage by canceling or freezing the card as soon as possible. Some banks let you do this with the click of a button in their mobile banking apps. Avoid simply tossing an old card in the trash. Shred or cut it first.

Card never arrived fraud is a low-tech version of a high-tech crime. Someone intercepts the card before it reaches you, such as from your mailbox. A lockable mailbox or renting a box at the post office are two ways to protect yourself.

False application fraud is the result of someone applying for a credit card in your name and running up debt that the fraudster has no intention of repaying, which can ruin your credit rating. Freezing your credit is a preventative measure, but it's probably also a good idea to monitor your bank accounts and protect sensitive information.

- **Social networks.** Since we're all friends on social networks, why wouldn't you respond to a friend's message? That's exactly what a hacker hopes you'll do after they break into someone's account and gain access to their contacts. The hacker then sends an urgent plea to those contacts, such as asking for cash or leading you to a link that installs viruses and other software that will corrupt your computer.

  To protect yourself, it's recommended to use different passwords for each social media network. Avoid clicking on unusual URLs sent through a social network. If you think something's amiss with a request you receive, you should contact the sender through another channel—such as a phone. You may also want to change the privacy settings of your social media account(s) so that only friends can see your personal information.

- **Phony office invoice.** Known as a fraudulent funds transfer scam, cybercriminals use social engineering to steal an email account from your organization. They then send you an email pretending to be an executive from your organization. This email can include an invoice and list bank account information, stating that you need to send a payment to the bank account as soon as possible.

  Confirm the legitimacy of an invoice before paying by contacting the person who allegedly sent the email. You may also want to verify the return address of the email.

- **This is tech support.** This rip-off usually begins with a phone call or pop-up warning on your device pretending to be from a legitimate tech company. The caller or pop-up warns that your computer has a virus or other problem. The tech impostor is hoping you will allow them to remotely access your computer.

  Generally, you should only use someone you know and trust to fix your computer. You should be suspicious if you are asked to pay with a gift card.

Fight back!

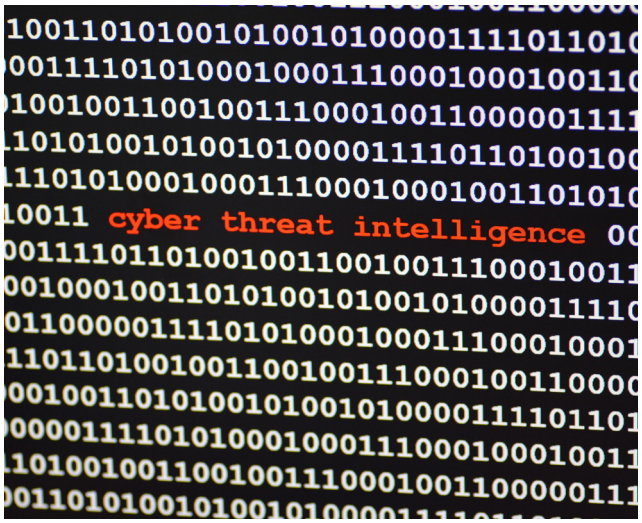
Recovering from identity theft/fraud can take months, which is why you should be aware of potential scams to protect yourself. But if the worst happens, you may be able to minimize the damage. Consider the following protection measures.

1. If you have identity theft insurance, file a claim.
2. Close any accounts that have been tampered with or opened fraudulently. Contact the fraud department at the business or bank where the fraudulent account was created and give them all pertinent information in writing. Follow-up to make sure accounts were closed and all requested actions were taken.
3. File a report with the Federal Trade Commission (identitytheft.gov).
4. Contact your local police department.
5. Place a fraud alert on your credit reports and freeze your credit for free through the credit bureaus at Equifax.com, Experian.com, and TransUnion.com.
6. Review your credit reports for mystery accounts.
7. Sign up for a credit monitoring service.
8. Change passwords and tighten security on your accounts.
9. Scan credit card and bank statements for unauthorized charges.

If You Become a Victim of Identity Theft

You should contact the fraud departments of the major credit bureaus immediately to let them know about your situation.

- **Equifax:** 800.525.6285; www.equifax.com; Fraud Victim Assistance Department, Consumer Fraud Division, P.O. Box 740256, Atlanta, GA 30374
- **Experian:** 888.EXPERIAN (397.3742); www.experian.com; National Consumer Assistance, P.O. Box 9554, Allen, TX 75013
- **TransUnion:** 800.680.7289; www.transunion.com; Fraud Victim Assistance Department, P.O. Box 2000, Chester, PA 19016-2000
- **Innovis:** 866.712.4546; www.innovis.com; Consumer Assistance, P.O. BOX 530086, Atlanta, GA 30353-0086



Also consider these protective measures:

- Request that these companies place a fraud alert in your file as well as a credit freeze. Order copies of your credit report from the credit bureaus to determine the extent of your victimization. Look for accounts opened and listed "inquiries." The listed inquiry gives you an indication of accounts opened or about to be opened. Several months later, request another credit report to confirm that the credit bureaus made the necessary corrections by removing the fraudulent accounts. This should also allow you to check for any other suspicious activity. Contact affected accounts for reporting, and order new cards and account numbers.
- Report the crime to the local police. This will establish the criminal activity and the facts. It is important that you obtain a copy of the report from the police because the credit bureaus, credit card companies, and other financial institutions may ask for a copy.
- File an identity theft complaint with the Federal Trade Commission (FTC) at identitytheft.gov.
- If you believe someone is using your SSN to work, get your tax refund, or other abuses involving taxes, contact the IRS at 800.908.4490 or visit them online at www.irs.gov/identity-theft-central. Ask whether you will require a new SSN.
- College students who have had their identification stolen should also contact the U.S. Department of Education (www.ed.gov/about/offices/list/oig/misused/index.html) for any college loans that may have been taken out with their identification.
- Visit the Internet Crime Complaint Center (www.ic3.gov), which is managed by the FBI and is a helpful source of ongoing scams.

AMG National Trust

A Better Way To Wealth

AMG helps executives, high net worth individuals, business owners, and institutions discover a better way to wealth. We work closely with you to develop integrated financial solutions customized to your unique goals and backed by our insightful research, thoughtful innovation, and decades of experience. Capitalize on your opportunities with a knowledgeable partner focused on your vision and your success.

Denver – *Corporate Headquarters*
6295 Greenwood Plaza Blvd.
Greenwood Village, CO 80111
800.999.2190
303.694.2190

Asheville – *Boys Arnold Office*
1272 Hendersonville Road
Asheville, NC 28803
800.286.8038
828.274.1542

Boulder – *Main Banking Office*
1155 Canyon Boulevard, Suite 310
Boulder, CO 80302
888.547.8877
303.447.8877

Cheyenne
Office hours by appointment only
1623 Central Avenue, Suite 106
Cheyenne, WY 82001
800.999.2190

Chicago
180 North LaSalle Street, Suite 2925
Chicago, IL 60601
877.662.8243
312.263.5235

Hilton Head – *Boys Arnold Office*
4 Dunmore Court, Suite 201
Hilton Head Island, SC 29926
866.422.1442
843.342.8800

Morristown
163 Madison Avenue, Suite 110
Morristown, NJ 07960
800.888.2777
973.455.0202

Virginia Beach
780 Lynnhaven Parkway, Suite 140
Virginia Beach, VA 23452
866.872.9578
757.368.4466

www.amgnational.com