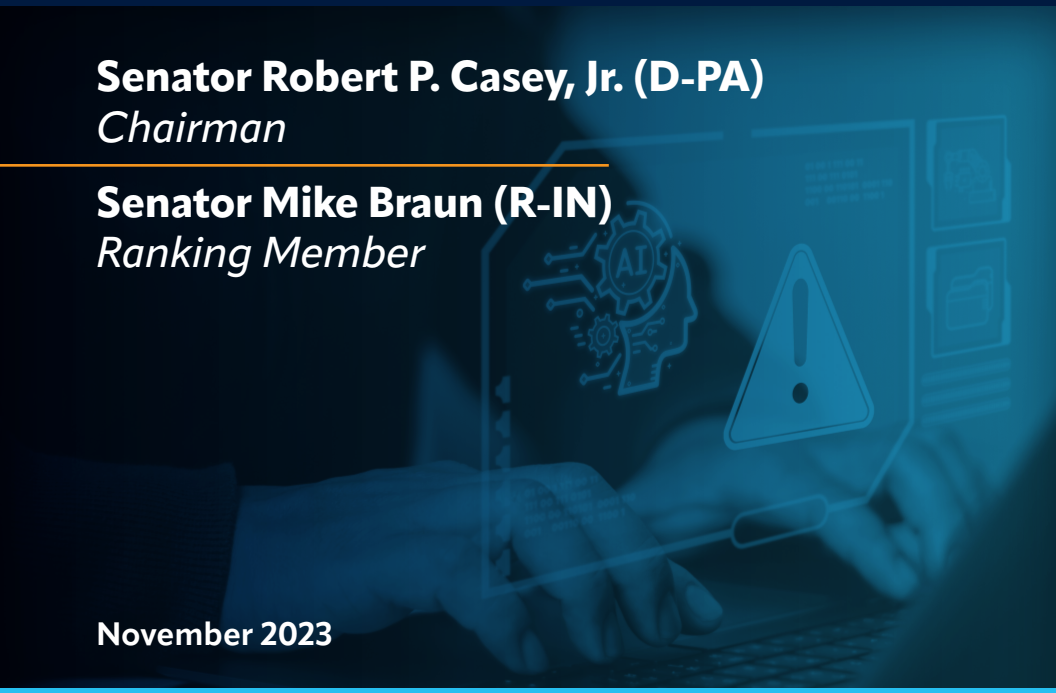
Fighting Fraud:

Top Scams in 2022

Senator Robert P. Casey, Jr. (D-PA)
Chairman

Senator Mike Braun (R-IN)
Ranking Member



November 2023

U.S. Senate
Special Committee on Aging

TABLE OF CONTENTS

About the Senate Special Committee on Aging

Established in 1961, the Special Committee on Aging is the focal point in the Senate for discussion and debate on matters relating to older Americans. The Aging Committee operates a toll-free Fraud Hotline (1-855-303-9470), which serves as a resource for older Americans and their family members to report suspicious activities and provides information on reporting frauds and scams to the proper officials, including law enforcement.

ROBERT P. CASEY, JR., Pennsylvania, CHAIRMAN

KIRSTEN GILLIBRAND, New York
RICHARD BLUMENTHAL, Connecticut
ELIZABETH WARREN, Massachusetts
MARK KELLY, Arizona
RAPHAEL WARNOCK, Georgia
JOHN FETTERMAN, Pennsylvania

MIKE BRAUN, Indiana, RANKING MEMBER

TIM SCOTT, South Carolina
MARCO RUBIO, Florida
RICK SCOTT, Florida
J.D. VANCE, Ohio
PETE RICKETTS, Nebraska

Learn more about our members and work at www.aging.senate.gov.

MESSAGE FROM CHAIRMAN CASEY AND RANKING MEMBER BRAUN

Dear Friends,

The U.S. Senate Special Committee on Aging (Committee) is committed to protecting older Americans against fraud and raising awareness to prevent scams.

This year, we celebrate 10 years of the Committee's Fraud Hotline. For the past decade, Committee staff operating the Fraud Hotline have provided callers with resources and guidance to help callers report incidences of fraud to the proper officials, such as law enforcement and government agencies.

Nearly 11,800 individuals from across the Nation have contacted the Committee's Fraud Hotline since its inception, including nearly 660 individuals in 2022. If you or a loved one need assistance connecting to resources or want to report suspicious activities that you think may be fraudulent, **contact the Committee's toll-free Fraud Hotline at 1-855-303-9470.** Committee staff are available to answer Monday through Friday, 9 AM to 5 PM Eastern Time.

In 2022, the top scam types reported to the Committee shared many similarities to those reported by the Federal Trade Commission (FTC): imposter scams and prizes, sweepstakes, and lottery scams are both cited as some of the top reported categories.[1]

Though many of the same types of scams present themselves year after year, the methods through which scammers contact victims have diversified—Artificial Intelligence (AI) and social media now play a prominent role.

The Committee has taken recent action to address this emerging fraud risk. In May 2023, the Committee sent a letter to FTC Chair Lina Khan requesting information on the rising prevalence of AI-powered technology in scams and how FTC is working to address these new AI-powered schemes. The Committee looks forward to working with FTC and other relevant agencies to safeguard older Americans from AI-related frauds and scams.

The Committee would like to thank the many consumer advocacy organizations, community centers, and local law enforcement officials that provide invaluable assistance to Americans on these issues. We hope this book can be used as a resource to help older adults respond to the most prevalent scams facing Americans today.

Sincerely,

Robert P. Casey, Jr.
Chairman

Mike Braun
Ranking Member

How Scammers are stealing people's money

To steal people's money, scammers utilize technology that allows them to reach thousands of people easily and cheaply, as well as payment methods that help them access the money quickly and leave no trace.

ALERT: Use of Artificial Intelligence in Scams

Artificial Intelligence (AI) is a newer technology that allows machines to mimic certain human-like behavior, such as speech or writing. For example, new chatbots and language processing tools can answer detailed questions, write compelling essays, and develop computer code. While this technology can be used for good, these powerful tools can also be exploited by bad actors to make scams more sophisticated and convincing than ever before. This section describes AI technology, how it can be used in frauds and scams, and what warning signs to look out for.

How is AI used?

- **Chatbots:** A chatbot is a computer program that simulates human conversation and is often used by companies to respond to customer inquiries. Some companies use AI technology in their chatbots to allow consumers to interact with the chatbots in a more natural way and, as a result, better respond to customer inquiries. Sometimes called virtual assistants, these AI-powered synthetic processors may have verified operators like Amazon's Alexa and Amtrak's Ask Julie. However, there are non-verified AI-powered chatbots, which could be used maliciously to obtain, store, and manipulate your personal data.

- **Voice Cloning Technology:** Voice cloning uses AI to create voice models that sound almost exactly like the real voice of someone you may know. Scammers only need a few seconds of audio to create these cloned voices. They can use these cloned voices to impersonate authorities or celebrities to ask for personal favors, money, or investment advice. They can also be used in "family emergency scams," which will be highlighted later in this section.
- **Deepfakes:** A deepfake is an AI-generated video or image that is made to look authentic. Fake images or videos can be used by scammers to manipulate their targets, utilize facial identification technology, and access personal data.

AI ACCELERATES THE EFFECTIVENESS OF PRE-EXISTING SCAMS

Here are the main AI-based scams to watch out for:

AI-Powered Phishing Attacks: Phishing attacks, where fraudsters deceive individuals into revealing sensitive information, have become increasingly sophisticated with the use of AI. Using AI-powered algorithms, scammers can quickly personalize phishing emails, imitate sophisticated dialogue, and bypass traditional spam filters, making it harder for individuals to distinguish between genuine and fraudulent communications.

Family Emergency Scams: In March 2023, FTC issued a warning about the increased use of AI in "family emergency" schemes, in which scammers convince targets that their family member is in distress to obtain cash or private information.[2] Scammers can utilize voice cloning and deepfakes to impersonate a loved one who claims they are in danger and needs money immediately; this type of scam can be extremely convincing and elicit fear in the target.

Romance Scams: Fraudsters employ AI to create and operate fake profiles on dating websites and social media platforms. These AI-generated profiles can appear genuine, often incorporating attractive deepfake photos and compelling personal details. AI-powered chatbots then simulate realistic conversation to build trust, with the goal of tricking the target into sending them money.

Tips to protect yourself:

- Scammers are skilled at using clever language to compel targets to share financial information, so any transaction request should be thoroughly verified.
  - Do not share sensitive information like your full name, home address, Social Security Number or Medicare Beneficiary Identifier, or banking information with an unverified contact.
  - Do not transfer or send money to unknown locations.

- Be careful what you download. Just like scammers, apps may claim to be something they are not and attempt to access your data or install malware on your device.
- Do not believe everything you see on the internet. If a video, call, picture, or message seems unusual or alarming, verify it with a trusted source or family member.
- Consider designating a "safe word" for your family that is only shared with your family members and close contacts. If you receive a call from a family member claiming to be in distress, you can ask for the safe word to ensure it is not an AI-generated voice clone.
- Do not provide any personal or sensitive information to an online chatbot. Any information you provide the chatbot should be treated like it is public information.

SPOTLIGHT ON PAYMENT METHODS: CRYPTOCURRENCY, PEER-TO-PEER (P2P) PAYMENTS, & GIFT CARDS

Cryptocurrency: The Federal Bureau of Investigations (FBI) found that adults ages 60 and older lost nearly $1.1 billion to scams involving cryptocurrency in 2022, a reported increase of nearly 350 percent from 2021.[3]

Cryptocurrency is a type of digital currency that generally exists only electronically. It is preferred by scammers because, like P2P payment apps, they get the money instantly, and the payments are typically not reversible. It also gives them pseudonymity. Cryptocurrency payments can be used in a variety of schemes from fake investment scams to romance scams.

Tips to protect yourself:

- Ignore requests to give out your private cryptocurrency keys. Those keys control your crypto and wallet access, and no one needs them in a legitimate cryptocurrency transaction.
- Ignore return on investment (ROI) claims that seem too good to be true.
- Do not engage with “investment managers” who reach out to you and make promises on ROI.
- A celebrity will not contact people directly to sell cryptocurrency. Do not respond to any messages purporting to be from a celebrity.
- Do not accept "free" cryptocurrency from strangers.
- Be Aware: No legitimate business will demand that you pay in cryptocurrency. This is always a scam.

To learn more about cryptocurrency and how to protect yourself from crypto-related scams, FTC has helpful information at https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams.

Peer-to-Peer (P2P) Payments: In 2022, FTC received more than 62,300 reports from consumers who sent money to fraudsters via P2P payment apps, like Cash App, Venmo, or Zelle, with reported losses totaling $163.5 million.[4] These P2P payment methods are often abused by scammers because they get the money instantly no matter their location, and many platforms do not allow for a transaction to be cancelled once money is sent.

Tips to protect yourself:

- Never send payments to someone you don't know. Take your time to be sure that you are sending money to the right person.
- Set up fraud alerts in your P2P payment app, or with the bank or credit card account that you linked to the app. Fraud alerts can let you know if personal information is changed or when transactions are made.
- P2P payment apps have social media elements, like lists of friends. Avoid sharing information like your address, phone number, and other personal details. As on social media, ignore friend requests from people you do not know.
- Any business that exclusively takes P2P payment apps or pre-paid debit card payments should be avoided.

- Like any other financial website, protect your account with a strong password. Use two-factor authentication.
- If you suspect you have been a victim of fraud, contact the P2P company and your bank and credit card company as soon as possible. They may be able to put a hold on the transaction and you may have some recourse if you did not authorize the transaction.

Gift Cards: Gift cards, along with credit cards and wire transfers, were some of the main payment methods used by scammers to request and steal money from older adults who reported a scam to the Committee's Fraud Hotline. When the victim sends the scammer the gift card number, the scammer immediately uses the balance, making it impossible to get the money back.

Tips to protect yourself:

- If you paid a scammer with a gift card, tell the company that issued the card right away.
- If you buy gift cards to give away or donate to family and friends, buy the gift cards from stores you know and trust. Check the protective stickers on the card to ensure that they do not appear to have been tampered with.
- Always keep your receipt. A receipt will help you file a report if you lose the gift card.
- Beware of the signs of scams, like requests to buy gift cards at several stores or to purchase a specific type of gift card.

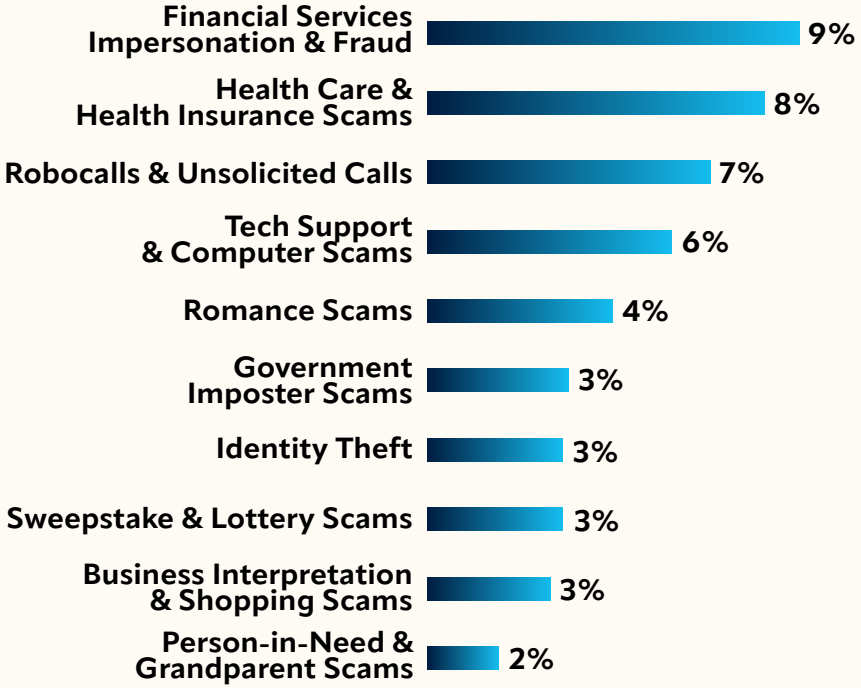
Top 10 Scams in 2022

In 2022, the Committee's Fraud Hotline received 659 new complaints from residents across the country. These complaints bring the total number of complaints registered with the Fraud Hotline since 2013 to nearly 11,800.

Figure 1 shows the Top 10 scams in 2022. These scams account for nearly half of all complaints reported to the Committee's Fraud Hotline in 2022. The other less common scams include home repair scams, utilities scams, and timeshare scams, among others.

For the first time since the Committee began operating the Fraud Hotline, Government Imposter scams are not the top type of scam reported to the Fraud Hotline.

FIGURE 1: TOP 10 SCAMS IN 2022



Note: This graph only represents the top 10 categories of scams, and therefore the percentages do not add up to 100 percent. In selecting the Top 10 categories, calls that were not related to a specific type of scam or fraud (e.g. requests for referrals and information from the Fraud Hotline) were excluded. Data for other categories can be found online at **https://www.aging.senate.gov/download/2022-fraud-book-additional-data**.

The Committee gathered additional details about the experiences of older adult victims. From this information we learned that, in 2022:

- **30 percent** of callers reported that they lost money or property;[5]
- **18 percent** of callers were concerned parties reporting fraud on behalf of an older adult.[6]

Aurelia Costigan

Bank Impersonation Scam Survivor

PITTSBURGH, PENNSYLVANIA

"Last September, I got a phone call from the number listed on the back of my debit card. This man said he was from Dollar Bank and that there were two suspicious activity charges on my account… he said he could help me… by adding a Zelle account that would protect my bank account…"

"He said, to know that he was actually speaking with Aurelia Costigan, he needed some form of identification… He asked [for] my Social Security Number. I assumed he was from my bank. He called from the right number…"

"About 5 to 10 minutes later, my phone starts blowing up. It's notifying me of charge after charge…Twenty-two, to be exact. I panicked, went to the bank… that's when I realized it was a scam."

"I was told to notify the police and file a complaint with the State Attorney's office…But I was absolutely a wreck. I couldn't sleep. I had trouble eating. I was just devastated. The money I lost – $1,800 – was a lot of money…I thought I was never going to get that money back."

"But thankfully, my bank was able to get my money back – the full $1,800. The State Attorney's office told me that I was very fortunate..."

"I know not everyone has that experience. These scammers get away with this every single day. Elderly people like myself, we are always the trusting type of people. But now, I tell people: don't give absolutely any information about yourself to anyone on the telephone. I hope that we can do something so that this doesn't happen to someone else."

Excerpts taken from Ms. Costigan's testimony provided to the Aging Committee in September 2022.

1. Financial Services Impersonation & Fraud

In 2022, the most common scam reported to the Committee's Fraud Hotline was financial services impersonation. As Ms. Costigan testified to in September 2022, scammers may impersonate financial services firms such as banks, debt collectors, or mortgage servicers.

For instance, scammers may pretend to be debt collectors and attempt to trick their targets into paying debts that do not exist. They may harass or threaten their intended victims with penalties or jail time if they refuse to pay. Mortgage relief scams involve promises related to refinancing and lies about the terms of a loan. According to FTC, in 2022 there were over 116,000 reported cases of debt collection fraud[7] and over 24,000 reported cases of mortgage fraud.[8] Fake bank fraud warnings were the most reported text message scam in 2022,[9] with a median reported loss of $3,000.[10]

RED FLAGS

These are common signs that you may be facing these types of scams:

Bank Impersonation Fraud

- You receive a text message, phone call, or email indicating that your account information has been compromised. They may ask for personal information like usernames, passwords, PINs, and Social Security Numbers to "secure" your account. They may also ask you to transfer funds using a P2P payment app, like Cash App, PayPal, Venmo, or Zelle.
- Banks will never contact you and ask you to share sensitive personal information over the phone, via text message, or email. They will never ask you to transfer money to anyone, including yourself, or ask you to provide personal information to obtain a refund or issue a correction.

Debt Collection Fraud

- The person calling you says you will go to jail if you don't pay the debt they are describing. It is illegal for debt collectors to threaten to have someone arrested for not paying their debts.
- The person calling will not tell you to whom you owe money. Legitimate debt collectors will always tell you who the creditor is, even if you don't ask them.
- Legitimate debt collectors provide ample time to pay off your debt and will work with you. Scammers will pressure you to pay while they have you on the phone.

Mortgage Relief Fraud

- The person calling and presenting the opportunity for a mortgage has not been referred to you by trusted friends and family.
- You are pressured into signing documents without the chance to consult an attorney.
- There are blank sections in the documents you are asked to sign. These blank sections can be filled out by the scammer after you've signed.
- You are pressured to pay up front before you get any services.

STEPS TO PREVENT AND RESPOND

Bank Impersonation Fraud

- Do not trust Caller ID. Scammers can "spoof" your Caller ID or falsify the information transmitted to your Caller ID so it hides their identity or allows them to impersonate a person or business.
- Do not click on links or respond to unexpected texts.
- If you receive a suspicious call, text, or email, hang up the call and don't respond to the text message or email. Call your bank or financial institution directly using verified contact information, such as the phone number on the bank's website or on the back of your bank card.

Debt Fraud

- Ask for a written debt validation letter. Debt collectors are obligated by law to send you detailed information about the debt you owe. Scammers will object to this request.
- Ask the person calling you for the collector's name and the name of the debt collecting agency they work for. If they say they are with law enforcement or an attorney, ask for their badge number, agency, or law firm. Scammers may object to or have trouble responding to these requests.

Mortgage Fraud

- Before signing any documents, consult with an attorney to be sure it is a legitimate mortgage. If the person attempting to get you to sign aggressively objects to you consulting an attorney, they may be a scammer.
- Be sure to carefully read any documents before signing. If you have questions, ask the person attempting to get you to sign. If they brush aside your concerns, they may be a scammer.

Report all suspicious calls or messages to FTC (1-877-382-4357) or your local law enforcement. You can also file a complaint online at https://reportfraud.ftc.gov/.

MORE INFORMATION

- The American Bankers Association has more information about bank impersonation scams at **https://www.banksneveraskthat.com/**.
- FTC provides more information about loans and debt-related scams at **https://consumer.ftc.gov/credit-loans-debt**.
- The Office of the Comptroller of the Currency (OCC) has more information about scams at **https://www.occ.treas.gov/topics/consumers-and-communities/consumer-protection/fraud-resources/index-fraud-resources.html**.

2. Health Care & Health Insurance Scams

Health care and insurance coverage decisions can be complex. Scammers take advantage of this complexity by impersonating the Medicare program, commercial health insurance plans, and health care providers, or by selling "discount health plans" that do not provide adequate coverage. They may also request personal or financial information "in exchange for" benefits. The Federal Communications Commission (FCC) finds that health-related scam calls targeted at older adults tend to spike during Medicare's open enrollment period, which runs from October to December.[11]

REPORTS FROM THE FRAUD HOTLINE

A man from Massachusetts received a call from a person claiming to represent the "Center for Medicare Verification Department," which does not exist. The caller told him he needed a new Medicare card; however, when asked for his employee identification number several times, the caller hung up.

RED FLAGS

These are common signs that you may be facing this type of scam:

- A caller posing as a government employee tells you that you will be charged a fee to obtain a Medicare card.
- You are asked via call, email, or text message for personal or financial information to "verify" your health insurance.
- You are offered help navigating the Health Insurance Marketplace – in exchange for a fee.
- You are offered a "discount" medical plan with little information and/or a lack of legitimate reviews online, and your doctor does not participate in the plan.
- You are given vague answers by a salesperson when you ask about specific details related to the insurance coverage the individual is selling.

STEPS TO PREVENT AND RESPOND

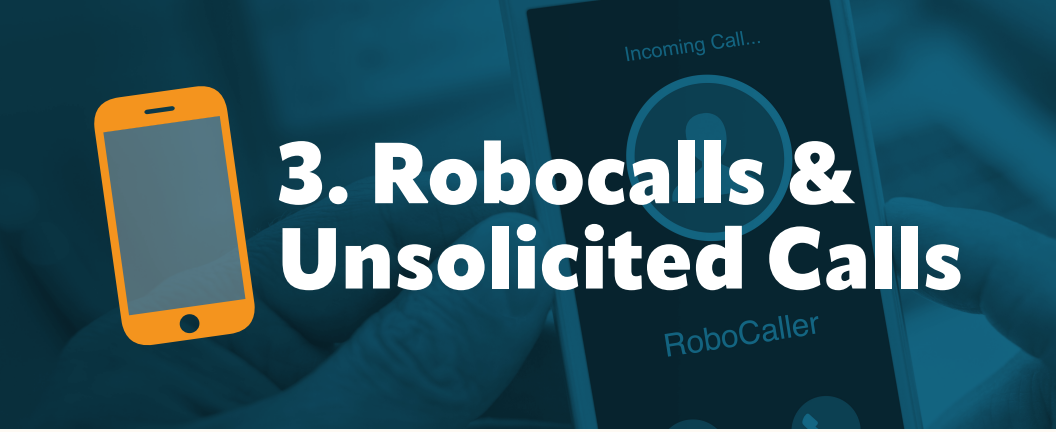
- Never give out personal information over the phone.
- Closely review all medical bills to spot any services that you did not receive. Reach out to your insurance provider to discuss.
- Visit trusted sources, like Healthcare.gov or Medicare.gov, to compare plans, coverage, and prices.

- Demand to see a statement of benefits or a complete copy of the insurance policy you are considering before making any decisions.
- Research any company offering health coverage, and if the salesperson claims the plan is provided through a major insurer, confirm directly with that insurer.
- Services offering legitimate help with the Health Insurance Marketplace, sometimes called "navigators" or "assisters," will not charge you. Go to **https://www.healthcare.gov/find-assistance/** directly for help. Those eligible for Medicare can find assistance with their State Health Insurance Assistance Programs (SHIPs) at **https://www.shiphelp.org/**.
- Report all suspicious calls or messages to FTC (1-877-382-4357) or your local law enforcement. You can also file a complaint online at **https://reportfraud.ftc.gov/**.

MORE INFORMATION

- FTC provides additional information and tips at **https://consumer.ftc.gov/articles/spot-health-insurance-scams**.
- FCC has more information on Medicare scams at **https://fcc.gov/older-americans-and-medicare-scams**.

- The Centers for Medicare & Medicaid Services (CMS) has resources for reporting scams or attempted scams at **https://www.medicare.gov/basics/reporting-medicare-fraud-and-abuse**.
- The U.S. Department of Health and Human Services maintains an extensive list of scam prevention information at **https://oig.hhs.gov/fraud/consumer-alerts/**.



3. Robocalls & Unsolicited Calls

Unwanted calls and robocalls are the top complaints that FCC receives,[12] and rank third in the most common complaints reported to the Committee's Fraud Hotline. Robocalls can be made from anywhere in the world and often contain a message from a prerecorded, robotic, or AI-generated voice. Robocallers may try to sell a product or service, and may "spoof," or imitate, a local number or a number for a business you are familiar with.

REPORTS FROM THE FRAUD HOTLINE

A woman from Maine received an unsolicited voicemail from someone claiming to be from her local police department. The caller said that her bank account will incur charges if she does not call back.

RED FLAGS

These are common signs that you may be facing this type of scam:

- You answer the phone and the caller – or a recording – asks you to hit a key to stop getting the calls. Scammers often use this trick to identify potential targets.
- You get an inquiry from someone who says they represent a company or government agency. When you hang up and call the verified phone number for that individual or organization, they have no record of calling you.

STEPS TO PREVENT AND RESPOND

- You may not be able to tell right away if an incoming call is spoofed. Be Aware: Caller ID showing a "local" number does not necessarily mean it is a local caller.
- Do not answer calls from unknown numbers.
- Do not respond to any unsolicited questions, especially those that can be answered with "Yes."
- Never give out personal information, such as account numbers, Social Security Numbers, maiden names, passwords, or other personally identifying information in response to unexpected calls, or if you are at all suspicious.
- If you experience fraud or monetary loss from a robocall, contact FCC at 1-888-225-5322 or FTC at 1-877-382-4357 as soon as possible. You can also file a complaint online at **https://reportfraud.ftc.gov/**.

MORE INFORMATION

- FCC has published tips to help consumers avoid spoofing scams at **https://www.fcc.gov/consumers/guides/spoofing-and-caller-id**.
- FTC provides helpful background on robocalls at **https://consumer.ftc.gov/articles/robocalls**.

Polly Fehler

Tech Support Scam Survivor

SENECA, SOUTH CAROLINA

"On April 13, I was using my new laptop on public Wi-Fi and suddenly a pop-up appeared on the home screen… alerting that my computer had been compromised…I immediately called the number on the screen."

"A reassuring voice alleging to be a representative of Microsoft answered. He told me to buy a protective software for $299..."

"I got another call from the same man who said that he was calling to check on the program…To run a test of the software, I had to give him full access. During this "test," messages flooded the screen. And, there it was again: An alert claiming my computer had been compromised…"

"Then… he opened a window showing my checking account… It had a balance of $26,000; $20,000 more than I should have… I had no idea where this money came from... The scammer was furious, demanding that if I didn't give the money back Microsoft would sue me …I was terrified."

"He told me to wire the $20,000 to a Microsoft subsidiary in Vietnam… After I completed the wire transfer, I called USAA… they told me… I had been scammed..."

"… After suffering through this scam, I was alone and depressed, even losing my spirit to live."

"I am here today because I'm a survivor… I hope we can prevent … others from falling into the darkness that comes with losing your self-worth and retirement savings in a click."

Excerpts taken from Ms. Fehler's testimony provided to the Aging Committee in September 2022.

4. Tech Support & Computer Scams

Computer-based scams involve con artists pretending to be associated with a well-known technology company, such as Microsoft, Apple, or Dell. As Ms. Fehler testified, they may use tactics like falsely claiming that an individual's computer has been infected with a virus or requesting the individual provide them with personal information and/or remote access to their computer. They may also request an individual's credit card or bank account number to "bill" for their services.

In a similar scam, the intended victim may see a pop-up window on their computer screen describing a security threat and instructing them to call a number for a tech support agent who is a scammer. FTC reports that in 2022, older adults were over six times more likely to report losing money to tech support scams than younger people.[13]

RED FLAGS

These are common signs that you may be facing this type of scam:

- You receive an alert saying there is a virus on your phone or computer and that you must call a number to resolve the issue.
- A scammer says that the only solution to protect your money or personal data from the "hacker" is to transfer your account funds to them while they get rid of the supposed virus.
- If you say that you would prefer to fix the issue by going to a physical store or calling a different company, the caller attempts to convince you that the virus is time-sensitive and only they can help you.

STEPS TO PREVENT AND RESPOND

- If you receive an alert saying your phone or computer has a virus, do not call the number provided in the alert. Instead, call the official tech support number for your device (e.g., Apple or Microsoft).
- If a person calls you saying your device has been hacked or compromised by a virus, hang up and block their phone number.
- Never provide personal or financial information to an unexpected caller.

- Do not give remote access to a device or account unless you contacted that company first and know it to be legitimate.
- Report all suspicious calls or messages to FTC (1-877-382-4357) or your local law enforcement. You can also file a complaint online at **https://reportfraud.ftc.gov/**.

MORE INFORMATION

- For more details about tech support scams, the Better Business Bureau has useful information at **https://www.bbb.org/article/news-releases/16553-bbb-tip-tech-support-scams**.

- FTC provides additional information on how to spot and avoid tech support scams at **https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams**.

5. Romance Scams

Social media, dating sites, and messaging apps are tools that scammers use to communicate with targets, build trust, and develop romantic relationships. These scammers target individuals seeking companionship and often quickly express their infatuation or love. They then may ask for money to pay for family issues, plane tickets, medical expenses, customs fees, or travel documents. The bad actor frequently "lives abroad." FTC reports that nearly 70,000 consumers reported they were victims of romance scams in 2022, with reported losses totaling $1.3 billion.[14]

REPORTS FROM THE FRAUD HOTLINE

A woman from Pennsylvania called the Fraud Hotline to report a romance scam that targeted her mother. The caller said her mother sent nearly $20,000 in gift cards to someone posing as Johnny Depp.

RED FLAGS

These are common signs that you may be facing this type of scam:

- The person never video calls you or meets you in person.
- You share no mutual friends with them on social media, and their identity is tough to trace online.
- They claim to be in love with you before meeting in person.
- They plan to visit you, but always have an excuse for why they can't that comes up last-minute.
- They request money be sent via cryptocurrency, wire transfer, or gift card.

STEPS TO PREVENT AND RESPOND

- If the person always refuses to video call or meet in person, block them.
- Never send money or gifts to someone that you have not met in person.
- Talk to your family and friends, or someone you trust, to get their advice.
- Contact your bank immediately if you think you sent money to a scammer.

- Report all suspicious calls or messages to FTC (1-877-382-4357) or your local law enforcement. You can also file a complaint online at **https://reportfraud.ftc.gov/**.

MORE INFORMATION

- The U.S. Secret Service provides tips on how to avoid romance scams at **https://www.secretservice.gov/investigation/romancescams**.
- FTC provides information and reporting resources at **https://consumer.ftc.gov/articles/what-know-about-romance-scams**.

6. Government Imposter Scams

Historically, government imposter scams were the top scam reported to the Committee's Fraud Hotline. In 2022, these scams were ranked sixth as scammers appear to be increasingly impersonating other entities such as businesses and financial institutions. In government imposter scams, bad actors will pretend to be a representative of a federal agency, such as the Social Security Administration (SSA) or Internal Revenue Service (IRS). They may threaten a person's benefits or demand payment for "taxes" or "fees." Among the different types of government imposter scams, Social Security related ones were the most common scam of this type reported to the Fraud Hotline.

REPORTS FROM THE FRAUD HOTLINE

A woman from Delaware reported that her ex-husband was contacted by a scammer impersonating a government agency. The victim was told his Social Security Number had been compromised, and he was instructed to send $22,000 to resolve the issue. The victim sent cash via UPS. Fortunately, the caller was able to contact UPS in time and stop the delivery.

RED FLAGS

These are common signs that you may be facing this type of scam:

- You receive a phone call, text, or email asking to confirm information that the government agency should already have, like an address or Social Security Number.
- The person contacting you threatens your benefits, asks you to wire money, put money on a prepaid debit card or gift card, or tells you to send cash or check using an overnight delivery service. They may also ask you to pay using cryptocurrency or via a P2P payment app.
- You are pressured to decide quickly and urgently, sometimes within a day or week.

STEPS TO PREVENT AND RESPOND

- Hang up the phone or do not reply to the email or text message.
- Never give out or confirm financial or other sensitive information in response to unexpected calls, or if you are at all suspicious.
- Do not inherently trust a name or number. Scammers may use official-sounding names to make you trust them. To make their call seem legitimate, scammers may also use technology to disguise their real phone number.
- A government agency will never ask you to wire money, provide your Social Security Number, or send funds via gift card.
- Call the federal agency directly and wait to speak to a customer service representative to verify the call or email you received.
- Report all suspicious calls or messages to FTC (1-877-382-4357) or your local law enforcement. You can also file a complaint online at **https://reportfraud.ftc.gov/**.

MORE INFORMATION

- FTC provides tips on how to spot and avoid imposter scams at **https://consumer.ftc.gov/features/imposter-scams**.

7. Sweepstake & Lottery Scams

Sweepstakes scammers intend to steal from older adults who believe they have won a lottery or a prize and only need to "take a few actions" to obtain their winnings. Often, a scammer will request that the individual pay a fee or tax to collect their winnings or improve their odds of winning. Scammers may instruct the individual not to share the news with anyone so it will be a "surprise" to their friends and family. They may also request money be sent via gift cards, wire transfer, P2P payment apps, money order, or cryptocurrency, in order to claim the prize. These payment methods are commonly used by scammers because it is difficult to get the money back once the transaction takes place. In 2022, FTC found that victims reported $302 million in losses to prize, sweepstakes, and lottery-related scams.[15]

REPORTS FROM THE FRAUD HOTLINE

A veteran from Georgia called the Fraud Hotline to report that he paid thousands of dollars to collect $1.2 million from a sweepstakes scam. He was told by the scammers that he would be refunded what he paid.

RED FLAGS

These are common signs that you may be facing this type of scam:

- You receive a call or message saying you have won a prize, but to claim the prize you must pay a "tax" or "processing fee."
- The person saying that you have won a prize tries to convince you that concerned family and friends are jealous or wrong.
- You are asked to pay the "tax" or "processing fee" by wiring money or sending money through the mail or via gift card, P2P payment apps, or cryptocurrency.
- You are told to lie to your bank about the reason for payment (e.g., "Tell your bank this money is for your sister.").

STEPS TO PREVENT AND RESPOND

- If you receive a call saying you have won a prize and the person calling mentions a "tax" or "fee," write down the number, hang up, and block the number.
- Do not respond to letters, texts, or emails saying you have won a prize, especially if it mentions a "tax" or "fee" to claim.
- Report any suspicious calls, messages, or mailers to FTC (1-877-382-4357) or your local law enforcement. You can also file a complaint online at https://reportfraud.ftc.gov/.

MORE INFORMATION

- The Better Business Bureau has tips on how to identify and avoid these scams at https://www.bbb.org/article/news-releases/16923-bbb-tip-sweepstakes-lottery-and-prize-scams.
- FTC provides more information on prize, sweepstakes, and lottery scams at https://consumer.ftc.gov/articles/fake-prize-sweepstakes-lottery-scams.

8. Identity Theft

Identity theft scams are when a bad actor wrongfully obtains and uses another individual's personal data. A common target for identity theft includes unauthorized access into a person's bank account. It may also include stealing Social Security Numbers, an individual's personal address, or even health care information. Fraudsters may withdraw money, input false applications for loans, or attempt to claim benefits like Social Security or unemployment on behalf of the older adult. In 2022, FTC took in more than 1.1 million reports of identity theft.[16]

REPORTS FROM THE FRAUD HOTLINE

A South Carolina woman contacted the Fraud Hotline to report that her personal information was being used in another state and someone was collecting income off it. She also reported that her credit score had dropped as a result.

RED FLAGS

These are common signs that you may be facing this type of scam:

- You receive an unsolicited call or message requesting personal information.
- You notice unusual activity on your credit report or bank account or new credit lines or loans in your name.
- You receive unfamiliar medical bills for procedures you did not receive or have inaccurate health conditions listed in your medical files.
- You do not receive the benefits, like Social Security or a tax refund, despite your account saying the funds were sent.

STEPS TO PREVENT AND RESPOND

- If someone asks you for your Social Security Number or personal information on the phone, hang up. If they claim to be from a legitimate company or agency, go to that organization's official website and call their official line to verify.
- Do not click on email links or open attachments, even if the message appears to be from a company you know. Doing so may put your personal information at risk. If you want to visit the website in the email, do so manually in a separate search tab.

- Update your passwords, especially if you suspect or learn that your bank or credit card company was breached. Do not use the same password across accounts.
- Subscribe to text and email alerts, especially those that inform you about unusual activity.
- Report all suspicious calls, messages, or mailers to FTC (1-877-382-4357) or your local law enforcement. You can also file a complaint online at **https://reportfraud.ftc.gov/**.

MORE INFORMATION

- More information on identity theft can be found on the Department of Justice's (DOJ) website at **https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud**.
- Report allegations of identity theft and find recovery resources at **https://www.identitytheft.gov**.

9. Business Impersonation & Shopping Scams

Scammers don't just impersonate government agencies; they can also impersonate businesses. These bad actors may claim there are unauthorized purchases or suspicious activity on an individual's account with their company. Business impersonators might also put fake phone numbers online for unknowing customers. Scammers request personal or financial information from the individual to "resolve" the issue and instead gain access to their account. According to FTC, in 2022, older adults reportedly lost $271 million to business impersonation scams, which is nearly 80 percent more than in 2021.[17]

REPORTS FROM THE FRAUD HOTLINE

A woman from New York received a call from her internet provider informing her that payment was past due. The caller hung up and contacted her internet provider directly, where she was informed that her account was current, and the call was likely a scam.

RED FLAGS

These are common signs that you may be facing this type of scam:

- When obtaining a refund, the caller says you need to provide them with remote access to your computer or account.
- A "business representative" tells you that too much money was "accidentally" refunded to your account and asks you to return the difference.
- You receive a call or email stating that unauthorized purchases were made on your account or that your account was hacked. The "business representative" says you will need to buy a gift card and send pictures of the numbers on the back to gain access to your account again.

STEPS TO PREVENT AND RESPOND

- Go to the company's website or your account directly to find contact information.
- Do not give remote access to a device or account unless you contacted that company first and know it to be legitimate.
- Legitimate businesses will never require you to pay exclusively via gift card, P2P payment apps, or cryptocurrency.
- Report any suspicious calls, emails, or mailers to FTC (1-877-382-4357) or your local law enforcement. You can also file a complaint online at **https://reportfraud.ftc.gov/**.

MORE INFORMATION

- FBI shares information on scammers posing as legitimate businesses at **https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise**.

10. Person-in-Need & Grandparent Scams

Bad actors may impersonate family members or friends in "person-in-need" or "grandparent" scams. Imposters may pretend to be a grandchild or a law enforcement officer detaining the individual's grandchild. They may also use AI to clone the voice of someone the individual knows to claim they are in trouble and need money to help with an emergency, like getting out of jail, paying a hospital bill, or leaving a foreign country. Scammers play on emotions and trick concerned family members into sending them money. The FBI reports that from January 2020 to June 2021, individuals reportedly lost $13 million to grandparent and person-in-need scams.[18]

REPORTS FROM THE FRAUD HOTLINE

A woman from Pennsylvania called the Fraud Hotline to report that she received a call from someone claiming to be her grandson. They said they were in a car accident and needed money to get home. The woman said that her grandson does not have a car, so she knew it was a scam and hung up the call.

RED FLAGS

These are common signs that you may be facing these types of scams:

- The person on the line asks you to send money immediately and shares specific details on how to do so. They may suggest you send the money via gift card or wire transfer.
- The "grandchild" or "law enforcement officer" on the line asks you to keep the incident a secret, despite the supposed urgency of the situation.
- The caller rushes you and asks you to make immediate decisions with little to no information.
- The caller reports to be in a situation or place that does not align with the typical behavior of the person they claim to be.

STEPS TO PREVENT AND RESPOND

- Hang up and call the number of your family member or a friend that you know to be genuine to ensure they are safe.
- If the person claims to be a law enforcement officer, hang up and call the relevant law enforcement agency to verify the person's identity and any information shared. Be Aware: Law enforcement will never contact a family member to collect bail money on behalf of someone else.
- Verify the story with trusted family and friends, even if you have been told to keep it a secret.

- Check your social media privacy settings and limit what information you share online. Criminals may try to use personal details to better target their scam and make it all the more convincing.
- Report all suspicious calls or messages to FTC (1-877-382-4357) or your local law enforcement. You can also file a complaint online at https://reportfraud.ftc.gov/.

MORE INFORMATION

- To handle these calls, FTC has helpful tips at https://www.consumer.ftc.gov/articles/0204-family-emergency-scams.
- FCC provides more information on how to avoid these scams at https://www.fcc.gov/grandparent-scams-get-more-sophisticated.
- To learn more about how AI is used in these types of scams, FTC has helpful information at https://consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes.

The Hotline Over the Years:

The Evolution and Diversification of Fraud Hotline Calls Over the Past Decade

In the past 10 years, the Committee has received nearly 11,800 calls to the Fraud Hotline, held 22 hearings examining frauds and scams, released 7 Fraud Books, and passed 4 pieces of legislation to address frauds and scams that target older adults, including the *Stop Senior Scams Act* and the *Senior Safe Act*.

While scams are constantly evolving, utilizing new technology, and developing new ways to steal your money, many of the top scams reported to the Fraud Hotline continue to present themselves year after year.

This is best captured in the reports the Fraud Hotline has received over the past 10 years, some of which are shown below. For many of these calls, the payment or contact method has changed, but the scam has largely stayed the same.

In 2013 and 2014, for example, scammers used methods like a prepaid debit card to obtain funds from victims. Now, scammers also use P2P payment apps, gift cards, and cryptocurrency to steal money. Scammers are also increasingly using AI technology to target and compel potential victims. It is often difficult for victims to know if they were scammed with the help of AI, but generally, the technology has made traditional scams, like grandparent scams and imposter scams, more convincing, and easier and cheaper for the scammer to deploy.

Government Imposter Scams Then and Now:

In 2014, a woman from Missouri reported that her mother was contacted by a door-to-door salesman. The caller's mother was told that she could sign up to have a doctor come to her home and educate her on the services Medicare provides. The caller's mother signed some forms and provided her Social Security Number and Medicare Beneficiary Identifier to the scammer.

In 2021, a man from Massachusetts received a recorded message claiming that his Social Security Number had been compromised. When he spoke to the person claiming to be from SSA, the caller requested the last four digits of his Social Security Number. The man asked multiple times for the caller's SSA employee ID number, and the scammer eventually hung up.

Romance Scams Then and Now:

In 2014, a caller reported that she was scammed out of $1,500 by a man she met on eHarmony [online dating site]. The scammer also asked the caller to open a bank account and provide him with the account information so he could make her a beneficiary for some gold he reportedly found.

In 2022, a caller from Mississippi reported that her mother met a man on Facebook and began communicating with him via Facebook Messenger. The scammer claimed that he was stationed overseas and couldn't access his money. The caller's mother had been sending him gift cards.

Business Impersonation Scams Then and Now:

In 2013, a caller reported that he was contacted via phone by a scammer impersonating UPS. The scammer told the caller that UPS was trying to deliver a packet from the IRS, but there was postage due. The caller hung up. The scammer called back and left a message telling the caller to buy a pre-paid money card to pay the postage and mail it to Florida.

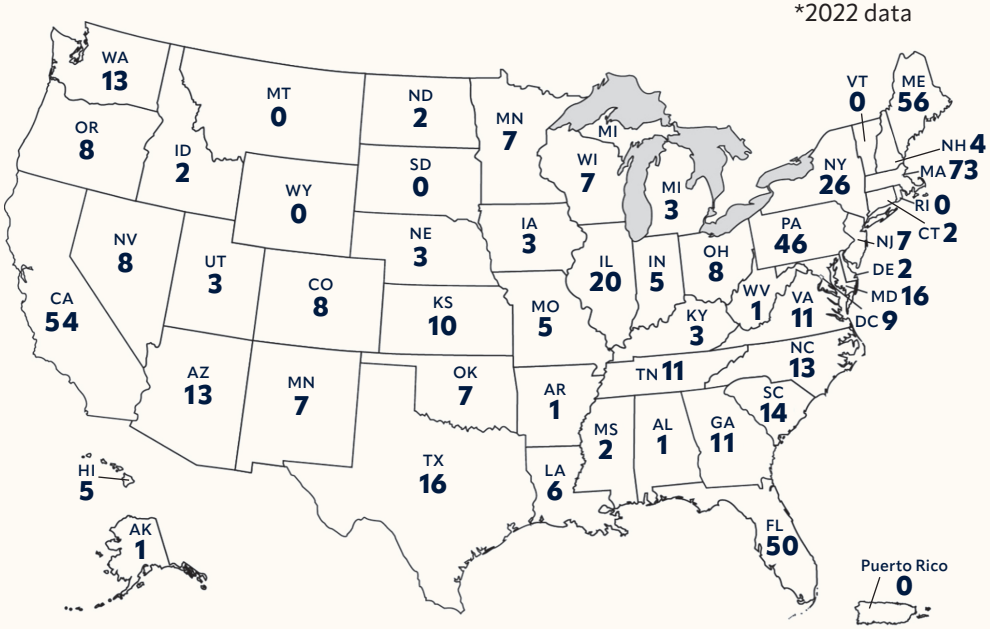
In 2022, a man from Minnesota said that he was contacted by a scammer via text message. The scammer claimed to be an employee with Amazon and said that the caller had to update his Amazon Prime membership, or he would lose access. The caller paid $159.99 through PayPal [P2P payment app]. The caller realized it was a scam and was able to cancel the payment.

The Committee has demonstrated a steadfast commitment to educating consumers about the everchanging methods fraudsters utilize and will continue to look for opportunities to get ahead of scammers' new technology.

Scams by State

NUMBER OF COMPLAINTS REPORTED TO THE FRAUD HOTLINE BY STATE*:

*2022 data



State	2015 - 2021	2022	Total
Alabama	95	1	96
Alaska	19	1	20
Arizona	186	13	199
Arkansas	40	1	41
California	576	54	630
Colorado	71	8	79
Connecticut	48	2	50
Delaware	33	2	35
District of Columbia	15	9	24
Florida	502	50	552
Georgia	83	11	94
Hawaii	16	5	21
Idaho	20	2	22

State	2015 - 2021	2022	Total
Illinois	143	20	163
Indiana	58	5	63
Iowa	135	3	138
Kansas	32	10	42
Kentucky	45	3	48
Louisiana	33	6	39
Maine	2,596	56	2,652
Maryland	483	16	499
Massachusetts	114	73	187
Michigan	134	3	137
Minnesota	59	7	66
Mississippi	18	2	20
Missouri	59	5	64
Montana	22	0	22
Nebraska	27	3	30
Nevada	38	8	46
New Hampshire	32	4	36
New Jersey	118	7	125
New Mexico	32	4	36
New York	468	26	494
North Carolina	97	13	110
North Dakota	10	2	12
Ohio	136	8	144
Oklahoma	38	7	45
Oregon	61	8	69
Pennsylvania	655	46	701
Rhode Island	79	0	79
South Carolina	73	14	87
South Dakota	16	0	16

State	2015 - 2021	2022	Total
Tennessee	77	11	88
Texas	573	16	589
Utah	74	3	77
Vermont	6	0	6
Virginia	175	11	186
Washington	141	13	154
West Virginia	36	1	37
Wisconsin	55	7	62
Wyoming	12	0	12
Puerto Rico	1	0	1
Outside the U.S.	1	0	1
Unknown	403	79	482
All Areas	**9,069**	**659**	**9,728***

Note: While the Fraud Hotline was established in 2013, the data collected in 2013 and 2014 is incomplete and incompatible with the data collected from 2015 through 2022. For that reason, the Committee chose not to incorporate it into this analysis. The number of calls are not a statistically representative measure of the incidence of scams or financial exploitation of older adults in each state. Calls to the Fraud Hotline are likely reflective of consumer awareness of the Fraud Hotline in each state/jurisdiction.

**There were an additional 2,057 complaints submitted to the Fraud Hotline in 2013 and 2014.*

Resources

ADDITIONAL TIPS ON HOW TO PROTECT YOURSELF FROM DIFFERENT CONTACT METHODS USED BY SCAMMERS

TEXT MESSAGES, ONLINE POP-UPS, & SOCIAL MEDIA

Text Messages: Scammers will often use text message scams to impersonate well-known businesses, such as a bank or a package delivery service. They could promise a gift, prize, or job. One thing is certain: these scammers are trying to take your money and personal information.

Tips to protect yourself:

- If you receive an unexpected text from an unknown sender, do not click on any links or respond to the message. If you think the text message is legitimate, contact the company directly; do not use the contact information provided in the text message.
- Do not pay to have a package redelivered. Package delivery companies will never request payment to redeliver a package.
- You can report these text scams by forwarding them to 7726 (SPAM). This can help your cell phone provider identify and block similar spam messages.

Pop-Up and Online Ads: Pop-ups are a common strategy used by "tech support" scammers, which are discussed earlier in this book.

Online ads are used to impersonate legitimate businesses and retailers. These ads often advertise deals that are "too good to be true." Scammers steal the victim's information, like a credit card number, once they make the purchase.

Tips to protect yourself from fraudulent online ads and pop-ups:

- Do not click on any links from website pop-ups and online ads. To visit a website, type the website address directly into the browser.
- Back up your data regularly. Backups may be the best way to recover your information and files if your computer is infected with a virus or ransomware.
- Do not download software from sites you don't know.
- Authorize your anti-virus and anti-malware software to update automatically and regularly scan your computer for viruses and malware.

Social Media: Social media is one of the most common contact methods used by scammers targeting older adults online and offers scammers an opportunity to access personal details and gain the trust of the target.

Tips to protect yourself from bad actors on social media:

- Be sure to use a strong password and privacy settings that hide information like your city, phone number, and date of birth.
- Do not accept friend requests from strangers, from someone you already have as a "friend" on social media, or from someone that you know does not use social media.
- Do not click on links sent by friends with whom you normally do not communicate. These links are usually to a website to claim a prize, take a quiz, fill out a survey, or watch a video.
- Confirm with a friend or contact, or meet them in person, if you get an urgent online request from them for money or an investment. Be Aware: Their account may have been hacked, especially if they ask you to send cryptocurrency, gift cards, or a wire transfer.

ADDITIONAL RESOURCES FROM AGENCIES & OTHER ORGANIZATIONS

These organizations and websites can serve as a resource for consumers and may include information on other common scams that target older adults that are not covered in this book.

Entity	Website
Better Business Bureau (BBB)	https://www.bbb.org/scamtracker
AARP Fraud Watch Network	https://www.aarp.org/fraudwatchnetwork
Federal Trade Commission (FTC)	https://www.consumer.ftc.gov/scams
FBI	https://www.fbi.gov/scams-and-safety/common-scams-and-crimes
USA.gov	https://www.usa.gov/common-scams-frauds

REPORTING ELDER FINANCIAL ABUSE

The perpetrators of the scams discussed in this book are primarily strangers, often located in a different state or country than their victims. However, every year millions of older Americans are exploited by people known to them, whether by a family member, caregiver, friend, financial professional, or other trusted person. Many older adults who are financially abused are also abused in other ways.

- If you know someone who is at immediate risk, call **9-1-1.**
- Report the incident to Adult Protective Services (APS). Use the National Adult Protective Services Association (NAPSA) list to find the phone number of the APS in your area **https://www.napsa-now.org/aps-program-list/** or call **2-1-1.**
- If the abuse is taking place at a long-term care facility, such as a nursing home or assisted living facility, a long-term care ombudsman can help. Use the Consumer Voice National Long-Term Care Ombudsman Resource Center interactive map to find a Long-Term Care Ombudsman Program in your area: **https://theconsumervoice.org/get_help**.
- Contact your U.S. Congressperson or U.S. Senator. You can report the fraud to their office, and they may be able to provide assistance. To locate your Congressperson using your zip code, go to **https://www.house.gov**. To locate your Senator, go to **https://www.senate.gov/senators/senators-contact.htm**. You can also call **(202) 224-3121**. A switchboard operator will connect you directly with the office you request.

GETTING HELP AFTER A SCAM

Scams affect the financial, emotional, and physical health of the victims and their families. There are resources to help you respond and recover from fraud.

Victim support and counseling

Resource: VictimConnect Resource Center

Website: https://victimconnect.org/

Phone: 1-855-484-2846

Legal help

Resource: Legal Services Corporation

Website: https://www.lsc.gov/about-lsc/what-legal-aid/get-legal-help

Phone: Use the search tool to find the phone number for the local legal aid office

For other services

Resource: Eldercare Locator

Website: https://eldercare.acl.gov/

Phone: 1-800-677-1116

STATE ATTORNEYS GENERAL

You can call your Attorney General's office at:

STATE/TERRITORY	PHONE NUMBER
Alabama	(334) 242-7300
Alaska	(907) 269-5100
American Samoa	(684) 633-4163
Arizona	(602) 542-5025
Arkansas	(800) 482-8982
California	(916) 445-9555
Colorado	(720) 508-6000
Connecticut	(860) 808-5400
Delaware	(302) 577-8600
District of Columbia	(202) 442-9828
Florida	(850) 414-3300
Georgia	(404) 651-8600
Guam	(671) 475-2720
Hawaii	(808) 586-1500
Idaho	(208) 334-2400
Illinois	(312) 814-3000
Indiana	(317) 232-6330
Iowa	(515) 281-5926
Kansas	(785) 296-3751

STATE/TERRITORY	PHONE NUMBER
Kentucky	(502) 696-5300
Louisiana	(225) 326-6465
Maine	(207) 626-8800
Maryland	(410) 576-6300
Massachusetts	(617) 727-2200
Michigan	(517) 335-7622
Minnesota	(651) 296-3353
Mississippi	(601) 359-3680
Missouri	(573) 751-3321
Montana	(406) 444-2026
Nebraska	(402) 471-2682
Nevada	(702) 486-3132
New Hampshire	(603) 271-3658
New Jersey	(609) 292-8740
New Mexico	(505) 490-4060
New York	(518) 776-2000
North Carolina	(919) 716-6400
North Dakota	(701) 328-2210
Northern Mariana Islands	(670) 237-7600
Ohio	(614) 466-4986
Oklahoma	(405) 521-3921

STATE/TERRITORY	PHONE NUMBER
Oregon	(503) 378-4400
Pennsylvania	(717) 787-3391
Puerto Rico	(787) 721-2900
Rhode Island	(401) 274-4400
South Carolina	(803) 734-3970
South Dakota	(605) 773-3215
Tennessee	(615) 741-3491
Texas	(512) 463-2100
US Virgin Islands	(340) 774-5666
Utah	(800) 244-4636
Vermont	(800) 649-2424
Virginia	(804) 786-2071
Washington	(360) 753-6200
West Virginia	(304) 558-2021
Wisconsin	(608) 266-1221
Wyoming	(307) 777-7841

You can also contact your Attorney General online. The National Association of Attorneys General provides an up-to-date list of all state Attorney General websites at: **https://www.naag.org/find-my-ag/**.

THREE STEPS TO HELP YOURSELF AND HELP OTHERS

Spread the word

- Talk to family, friends, and neighbors.
- Share this fraud book and what you have learned with others.

Report the scam

- To the authorities: your information can help identify and locate scammers.
- To the companies involved: they are also often victims and can help fight scammers along with you.

Stay alert and be proactive

- Consider signing up for alerts from your bank and credit card company, or a credit monitoring service.
- Safeguard your online information by using different and strong passwords for your accounts. Use two-factor authentication when available.
- Utilize the tools and tips provided in this book.

U.S. SENATE
SPECIAL COMMITTEE ON AGING

Fraud Hotline

The Fraud Hotline serves as a resource for older Americans and their family members to report suspicious activities and to obtain information on reporting frauds and scams to the proper officials, including law enforcement.

1-855-303-9470

MON – FRI

9 AM to 5 PM ET

NOTE & REPORT CHECKLIST

This information can help you report the incident to agencies and companies.

Acting soon is important. Do not wait to have all of this information before reporting.

	Important information to include in your complaint	Your notes
☐	When did it happen?	
☐	How were you contacted?	
☐	What were you asked to do?	
☐	How much money were you asked to provide?	

☐	How were you asked to provide the money?	
☐	Where did the person say they were located?	
☐	Did you report the incident to the implicated business or the financial institution?	
☐	Did you report this incident to anyone else?	
☐	Was any of the money you sent refunded?	
☐	Was there any other effect (account closed, ID theft)?	

Disclaimer: The Fraud Book provides general consumer information about frauds and scams. This information may include links to third-party resources or content. The Committee does not endorse any third-party. There may be other resources that also serve your needs.

ENDNOTES

1 Federal Trade Commission (FTC), "FTC crunches the 2022 numbers. See where scammers continue to crunch consumers," https://www.ftc.gov/business-guidance/blog/2023/02/ftc-crunches-2022-numbers-see-where-scammers-continue-crunch-consumers (last visited October 22, 2023)

2 FTC, "Scammers use AI to enhance their family emergency schemes," https://consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes (last visited October 22, 2023)

3 Federal Bureau of Investigations (FBI), Elder Fraud Report 2022, pg 9, https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3ElderFraudReport.pdf (last visited November 3, 2023)

4 Analysis of FTC data by Aging Committee staff. The analysis includes total complaints for all ages in 2022. FTC data is available online at: https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods (last visited October 22, 2023)

5 This analysis was conducted by Aging Committee staff and included individuals who did not respond to questions regarding loss of money or property.

6 This analysis was conducted by Aging Committee staff and included individuals who did not disclose their relationship to the victim.

7 FTC, Explore Debt Collection Reports, https://public.tableau.com/app/profile/federal.trade.commission/viz/DebtCollection/Infographic (last visited October 22, 2023)

8 FTC, Consumer Sentinel Network Data Book 2022, pg 7, https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf (last visited October 22, 2023)

9 FTC, "New FTC Data Analysis Shows Bank Impersonation is Most-Reported Text Message Scam," https://www.ftc.gov/news-events/news/press-releases/2023/06/new-ftc-data-analysis-shows-bank-impersonation-most-reported-text-message-scam (last visited October 22, 2023)

10 FTC, "IYKYK: The top text scams of 2022," https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/06/iykyk-top-text-scams-2022 (last visited October 22, 2023)

11 Federal Communications Commission (FCC), "Health Care Scams Tend to Spike During Open Enrollment," https://www.fcc.gov/health-care-scams-tend-spike-during-open-enrollment (last visited October 22, 2023)

12 FCC, "Stop Unwanted Robocalls and Texts," https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts (last visited October 22, 2023)

13 FTC, "FTC Issues Annual Report to Congress on Agency's Actions to Protect Older Adults," https://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-issues-annual-report-congress-agencys-actions-protect-older-adults (last visited October 22, 2023)

14 FTC, "Romance scammers' favorite lies exposed," https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed (last visited October 22, 2023)

15 FTC, Consumer Sentinel Network Data Book 2022, pg 8, https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf (last visited October 22, 2023)

16 FTC, Protecting Older Consumers 2022-2023, pg 25, https://www.ftc.gov/system/files/ftc_gov/pdf/p144400olderadultsreportoct2023.pdf (last visited October 27, 2023)

17 FTC, "FTC Issues Annual Report to Congress on Agency's Actions to Protect Older Adults," https://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-issues-annual-report-congress-agencys-actions-protect-older-adults (last visited October 22, 2023)

18 FBI, "FBI Miami Warns of Grandparent Fraud Scam," https://www.fbi.gov/contact-us/field-offices/miami/news/fbi-miami-warns-of-grandparent-fraud-scheme (last visited October 22, 2023)

Notes

Notes

Notes

Notes

Fraud Hotline

1-855-303-9470

U.S. Senate
Special Committee on Aging