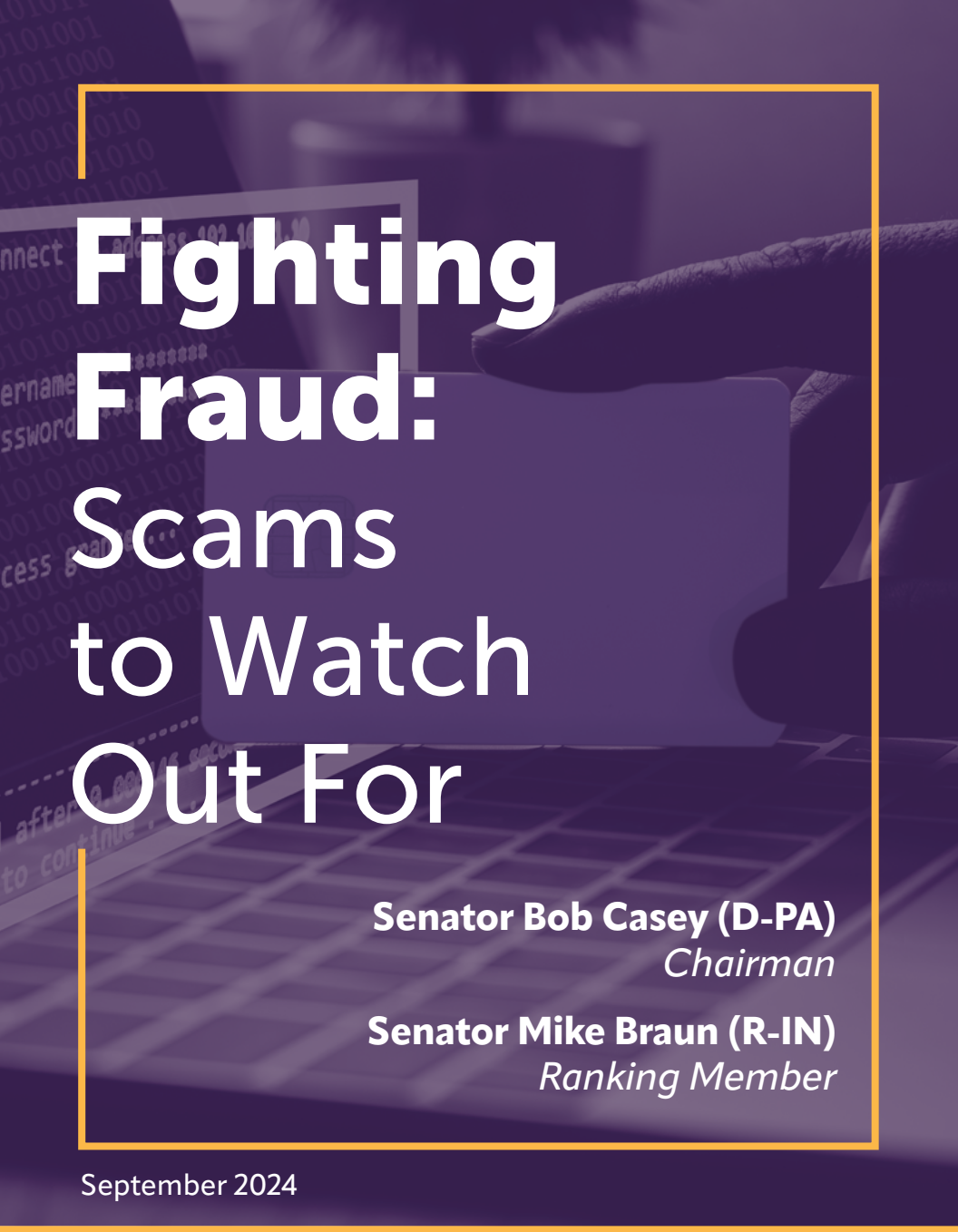


Fighting Fraud: Scams to Watch Out For

Senator Bob Casey (D-PA)
Chairman

Senator Mike Braun (R-IN)
Ranking Member

September 2024

U.S. Senate
Special Committee on Aging

TABLE OF CONTENTS

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 provides information for older Americans and their family members on how to identify scams and report fraud and scams to the proper officials, including law enforcement.

BOB CASEY, 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 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.

The Committee maintains a toll-free Fraud Hotline where Committee staff provide callers with resources and guidance to help callers report incidences of fraud to the proper officials, such as local law enforcement and federal agencies like the Federal Trade Commission (FTC), the Department of Justice (DOJ), and the Federal Bureau of Investigation (FBI), among others.

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 Monday through Friday, 9 AM to 5 PM Eastern Time.

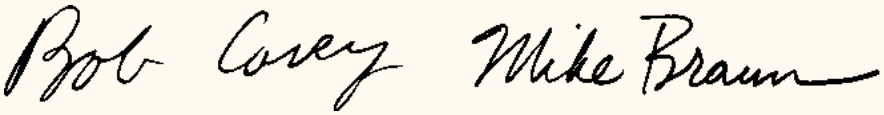
In 2023, many of the scams reported to both the Committee's Fraud Hotline and FTC were similar to those reported the year prior: imposter, sweepstakes, and lottery scams were cited as some of the top reported categories in both years. Scams involving technology, including cryptocurrency, Artificial Intelligence (AI), and social media, continue to play a significant role. In 2023, the three payment methods used by scammers where consumers lost the most money were bank transfers, cryptocurrency, and wire transfers.[1]

While the types of scams remain relatively the same year over year, losses are on the rise. FTC reports that in 2023, losses topped $10 billion—$1 billion more than those reported in 2022, and the highest losses ever reported to FTC.[2]

The Committee continues its work to educate and raise awareness of schemes targeting older adults, particularly those that are on the rise. In November 2023, the Committee held a hearing entitled, *Modern Scams: How Scammers Are Using Artificial Intelligence & How We Can Fight Back*.[3] This hearing focused on the threat posed by AI-powered scams and the ways this technology could be used to combat fraud. One witness, Gary Schildhorn, a lawyer from Philadelphia, told his story of nearly being scammed out of $9,000 through an AI-powered voice-cloning scheme. You can read more of Gary's story on page 25.

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 and others respond to the most prevalent scams facing Americans today.

Sincerely,



Bob Casey
Chairman

Mike Braun
Ranking Member

Financial Exploitation

Every year millions of older Americans are financially exploited by people known and unknown to them. According to the National Adult Protective Services Association (NAPSA), elder financial exploitation is the misuse, mishandling, or exploitation of property, possessions, or assets of older adults. This is often without the older adult's consent, under false pretense, or through undue influence, coercion, or manipulation.[4] Perpetrators of elder financial exploitation range from family members and other trusted individuals to professional criminals and scammers.

A recent analysis by the U.S. Department of the Treasury's Financial Crimes Enforcement Network found that between June 2022 and June 2023, there were more than 155,400 bank filings, worth a total of $27 billion, where elder financial exploitation was suspected.[5]

While people of all ages can be victims of financial exploitation, older adults are often targeted as they are more likely to have accumulated assets from decades of work and saving. Through elder financial

exploitation, many older adults are robbed of their retirement savings or funds saved for future medical and caregiving expenses. Elder financial exploitation can also lead to declines in mental and physical health.[6]

Financial exploitation, which is a form of elder abuse, is more common among older adults who are socially isolated, encounter barriers in accessing services, or experience cognitive impairment. It often goes unreported due to fear, embarrassment, or lack of resources.[7]

ELDER FINANCIAL EXPLOITATION GENERALLY FALLS INTO TWO CATEGORIES: THEFT AND SCAMS

Theft

Theft occurs when someone steals an older adult's assets, funds, or income. The perpetrator is usually a known and trusted person, such as a family member, caregiver, friend, financial professional, or business associate.

Examples of theft include forging checks, changing names on bank accounts, or using credit cards without permission.

Scams

Scams involve the transfer of money to a stranger or imposter for a promised benefit that the victim never receives. The perpetrators of scams are primarily strangers, often located in a different state or country than their victims.

Examples of scams include tech support scams, grandparent or person-in-need scams, and government imposter scams, which are all highlighted later in this book.

ELDER FINANCIAL EXPLOITATION CAN ALSO COME IN OTHER FORMS. IT INCLUDES:

- Coercing or deceiving an older adult into signing a contract, will, or other document.
- The improper use of a conservatorship, guardianship, or power of attorney.

Steps to Protect Yourself:

- Plan ahead to protect your assets and ensure your wishes are followed.
- Shred anything that has your personal information on it, including receipts, bank statements, mail, and even unused credit card offers before throwing them away.
- Lock up important financial and sensitive information when others are in your home.
- Do not allow others to have access to your financial information.
- Verify those you plan to hire by checking references and credentials.
- Regularly review your credit report.
- Never share personal information to anyone over the phone unless you initiated the call and know the communication to be legitimate. This information includes your Social Security Number, bank account number, or other sensitive information.

- Do not rush to make a financial decision. Consider a second opinion and request additional information in writing.
- Consult with a professional you trust, such as your financial advisor or attorney, before signing something you don't understand.
- **Trust your gut:** If something doesn't feel right, it may not be right.

Reporting Elder Financial Exploitation

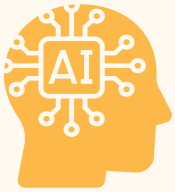
- If you, or someone you know, is at immediate risk, call **9-1-1.**
- Report the incident to your bank and local law enforcement.
- Report the incident to Adult Protective Services (APS). Use NAPSA's list to find the phone number of the APS in your area **www.napsa-now.org/aps-program-list/** or call **2-1-1.**
- File a report with FTC at **reportfraud.ftc.gov** or FBI at **ic3.gov**.
- Report it to DOJ's Elder Fraud Hotline at **833-FRAUD-11** (833-372-8311).
- If the abuse is taking place at a long-term care facility, such as a nursing home or assisted living facility, APS and long-term care ombudsmen can help. Long-term care ombudsmen are consumer advocates who ensure the rights and dignity of residents living in long-term care facilities.

Use the Consumer Voice National Long-Term Care Ombudsman Resource Center interactive map to find a Long-Term Care Ombudsman Program in your area: **theconsumervoice.org/get_help.**

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 and currency that help them access money quickly and leave no trace.

SPOTLIGHT ON TECHNOLOGY: ARTIFICIAL INTELLIGENCE



Artificial Intelligence (AI) is a 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. This section describes AI technology, how it can be used in fraud and in scams, and what warning signs to look out for.

How is AI used?

Chatbots: A chatbot is a computer program that may use AI to simulate human conversation and could be used maliciously to obtain, store, or manipulate your personal data.

Voice Cloning Technology: Voice cloning uses AI to create voice models that sound like the real voice of someone you may know.

Deepfakes: A deepfake is an AI-generated video or image that is made to look authentic.

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, 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 family emergency scams, scammers convince targets that their family member is in distress to obtain cash or private information. Scammers can utilize voice cloning and deepfakes to impersonate a loved one who claims they are in danger and needs money immediately.

Romance Scams: Fraudsters employ AI to create and operate fake profiles on dating websites and social media platforms. AI-powered chatbots then simulate realistic conversation to build trust, with the goal of tricking the target into sending them money.

It may be difficult to know if someone is using AI-technology in a scam. **One thing is certain: AI makes traditional frauds and scams more convincing and easier to deploy on a larger scale.**

Tips to protect yourself:

Do not share sensitive information via phone, email, text, or social media.

Do not transfer or send money to unknown locations.

Consider designating a “safe word” for your family that is only shared with family members and close contacts.

Do not provide any personal or sensitive information to an online chatbot.

Report potential scams to the authorities and the companies involved.

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

Cryptocurrency: Cryptocurrency is a type of digital currency that only exists electronically. Cryptocurrency transactions may not be mediated by a trusted third party, are pseudonymous, and are difficult to track, which can make this payment method a useful mechanism for fraudsters. It is also preferred by scammers because they get the money instantly, and the payments are typically not reversible.

Cryptocurrency payments can be used in a variety of schemes including fake investment scams and false friendship or romance scams. These scams may also be used together: cryptocurrency investment scams can begin with scammers initially hooking victims through a false romance, and then progress to requests for money for an alleged investment.

A common technique scammers use is to build a relationship with their victims over time, earning their trust and then convincing them to invest in a fraudulent scheme, which results in significant financial losses; this is referred to as a "confidence investment scam," which is discussed further in this book. Once the scammer has gained the trust of the victim, scammers pressure victims to "invest" in a specific cryptocurrency platform by promising high returns and using sophisticated tactics to create a

sense of legitimacy. In reality, the platform is fake and controlled by the scammers, who disappear with the "invested" funds once they have accumulated enough money from unsuspecting investors.

The Federal Bureau of Investigation (FBI) found that adults ages 60 and older lost nearly $1.7 billion to scams involving cryptocurrency in 2023, a reported increase of nearly 52 percent from 2022.[8] The FBI also found that the largest losses among older adults involving cryptocurrency were crypto-related investment scams with over $716 million in reported losses.[9]

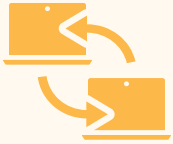
Tips to protect yourself:

- Ignore advice and offers to help you invest in cryptocurrency – it is most likely a scam.
- If you meet someone on a dating site or app, and they want you to send them cryptocurrency or show you how to invest in crypto, it is almost certainly a scam.
- 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.

- If you have been a victim of a cryptocurrency scam, be wary of anyone claiming they can recover your funds, as this could be another scam. Scammers often target the same person more than once because they perceive them as vulnerable, trusting, and potentially less likely to report the fraud or seek legal recourse after the initial victimization.
- **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, the FTC has helpful information at **consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams.**

The FBI has also released guidance for cryptocurrency scam victims, which can be found here: **www.ic3.gov/Media/Y2023/PSA230824**.



Peer-to-Peer (P2P) Payments: P2P payments are transactions between two parties with separate bank accounts, mediated through a third-party website or mobile app. These platforms can be abused by scammers because, like cryptocurrency, scammers receive the money instantly after a transfer is initiated. While many P2P payment companies employ advanced systems to flag and freeze suspicious transactions, these platforms are often unable to reverse a transaction once money is sent. These apps may also lack the same protections against fraud that traditional banks and credit cards now employ.

In 2023, the FTC received more than 65,300 reports from consumers who sent money to fraudsters via P2P payment apps, like CashApp, Venmo, or Zelle, with reported losses totaling nearly $210 million.[10] These reports represent an increase of 5 percent since the year prior, but reported losses are 28 percent higher than those reported in 2022.[11]

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.

Gift Cards: Gift cards continue to be primary methods used by scammers to request and steal money from older adults who reported scams 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.

In 2023, the FTC received more than 41,600 reports of gift card scams, resulting in nearly $217 million in reported losses.[12]

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 and a copy of the gift card. The number on the gift card and the store receipt will help you file a report if you lose the gift card or need to report a scam.
- Beware of the signs of scams, like requests to buy gift cards at several stores or to purchase a specific type of gift card.

- **Be aware**: No business or government agency will ever tell you to buy a gift card to pay them. This is always a scam.

For more information on gift card scams and how to protect yourself, visit the FTC at **consumer.ftc.gov/articles/avoiding-and-reporting-gift-card-scams**.

Scams to Watch Out For

In 2023, the Committee's Fraud Hotline received 536 new complaints from individuals across the country. These complaints bring the total number of complaints registered with the Fraud Hotline since 2013 to nearly 12,300.

Many of these frauds are also reported to the FTC. Through report collection, investigations, and other administrative actions, the FTC's Bureau of Consumer Protection stops unfair, deceptive, and fraudulent practices employed by both companies and individual scammers.

Reported frauds account for nearly 2.6 million of the 5.4 million complaints reported to the FTC in 2023.[13] Common fraud categories include imposter scams, online shopping and negative reviews, prizes and lottery scams, and investment-related fraud. Other less common, but still prevalent, scams include debt collection scams, mortgage scams, and home repair scams.[14]

IMPOSTER SCAMS

Imposter scams are the most pervasive of all scams reported to the FTC, with over 850,000 reports in 2023.[15] These scams can appear in many different forms as scammers find new ways to target victims. The next five sections will discuss some of the most prevalent imposter scams commonly used to target older adults.

SCAM SURVIVOR

Gary Schildhorn

Person-in-Need Scam Survivor

PHILADELPHIA, PENNSYLVANIA

"In February of 2020, I was driving to my office when my phone rang. It was my son, Brett. He was upset and crying. He told me he needed my help. He said [he] was in a car accident, and he was arrested. He said [he] may have a broken nose and his arm was hurt. The car he hit was purportedly driven by a pregnant woman who was injured. He reported that he was assigned a public defender named Barry Goldstein…I told him I would call Goldstein and call him right back. He said, "you can't, they took my phone, get me out, please."

I am a father and a lawyer. My son was hurt, he was in trouble and a pregnant woman was injured. This call instigated and required immediate action by me. I first

attempted to look up Mr. Goldstein. Before the search results came back, my phone rang. It was Mr. Goldstein. He told me he met with my son. He said Brett was hurt but was going to be okay.

He said the Judge had ordered a high bail of $150,000 and that I would need 10 percent of that amount in cash to bail him out... He asked if I was in a position to help my son. I assured him I was. He then… told me to call the court and arrange for bail... I called the number he provided. They answered, "Montgomery County Court House" …[and] confirmed they were holding my son… [They] also reported that…the judge …had lowered bail to $90,000.

[The Montgomery County Court House] then told me that in order to bail [my son] out I would have to use the county bail bondsman, but that there was a problem. The only bondsman available had a family emergency and was not in town…[They] suggested that I call Mr. Goldstein back because he would be able to assist. I placed the call.

Mr. Goldstein agreed to post a bond and informed me I would need to wire him $9,000. He stated he was a member of a credit union, and I would have to go to certain kiosks to wire the money. I later learned that these were bitcoin [a type of cryptocurrency] kiosks. He then told me that he was attending an out-of-town conference and would be leaving for the airport in two hours. I needed to hurry.

This series of calls all occurred within a few minutes. It was not until the calls stopped and I was driving to the bank that I had an opportunity to think. I called my daughter-in-law, Kim, told her what happened and asked her to alert my son's office that he had been in an accident.

A few minutes later, I received a Facetime call. It was Brett. "Dad, Kim called work and they put me on the phone." "You are being scammed; see, I'm fine." Shock, relief, and anger—one emotion followed the other. I said to Brett that there was no doubt in my mind that it was his voice on the phone—it was the exact cadence with which he speaks.… **How did they get my son's voice? The only conclusion I can come up with is that they used artificial intelligence, or AI, to clone his voice.**

Excerpts taken from Mr. Schildhorn's testimony provided to the Aging Committee in November 2023.

Person-In-Need & Grandparent Scams

As Gary testified in November 2023, 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 who has detained the target'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. Similar schemes can use the voices of nieces, nephews, children, or others. Between January and September 2023, the FBI's Internet Crime Complaint Center (IC3) received more than 195 reports regarding grandparent scams, resulting in at least $1.9 million in reported losses.[16]

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, wire transfer, or cryptocurrency.

- 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 the FTC (1-877-382-4357) or local law enforcement. You can also file a complaint online at **reportfraud.ftc.gov**.
- **Helpful Tip:** If you sent money to a scammer through a wire transfer, report it to the FBI's IC3 within 72 hours of the transfer at **ic3.gov**. They may be able to help recoup some of your lost funds.

MORE INFORMATION

- To handle these calls, the FTC has helpful tips at **www.consumer.ftc.gov/articles/0204-family-emergency-scams**.
- The FCC provides more information on how to avoid these scams at **www.fcc.gov/grandparent-scams-get-more-sophisticated**.
- The FBI released a public service announcement about these scams, which can be viewed at **www.ic3.gov/Media/Y2023/PSA231117**.
- To learn more about how AI is used in these types of scams, the FTC has helpful information at **consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes**.

Financial Services Impersonation & Fraud

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 the FTC, in 2023, there were over 124,400 reported cases of debt collection fraud and nearly 26,200 reported cases of mortgage fraud.[17] In 2022, fake bank fraud warnings were the most reported text message scam,[18] with a median reported loss of $3,000.[19]

Reports from the Fraud Hotline

A woman from Florida reported that she received a call from a scammer who was impersonating her bank. The scammer had spoofed the victim's Caller ID so it looked as if Bank of America was contacting her. The victim was then instructed by the scammer to send $950 through Zelle and CashApp.

BEWARE: PHISHING SCAMS

Phishing scams deceive people into giving away sensitive information by pretending to be legitimate organizations or businesses. Scammers use fake emails, text messages, or websites that mimic real ones, urging quick action through links or attachments. The data stolen through phishing is often used for identity theft or financial fraud. To protect yourself, verify the authenticity of unexpected messages, avoid suspicious links, and use strong and unique passwords.

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 unexpected 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 the FTC (1-877-382-4357) or local law enforcement. You can also file a complaint online at **reportfraud.ftc.gov**.

MORE INFORMATION

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

Tech Support & Computer Scams

Computer-based scams involve con artists pretending to be associated with a well-known technology company, such as Microsoft, Apple, Dell, or Best Buy's Geek Squad. 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. The FBI reports that in 2023, as in 2022, tech support scams were the top scam impacting older adult victims. Older adults reportedly lost nearly $590 million to tech support scams in 2023.[20]

Reports from the Fraud Hotline

A woman from Georgia called the Committee's Fraud Hotline to report that she lost $25,000 in a tech support scam. The caller reported that her computer had frozen and a pop-up appeared, which prompted her to call, what she believed, was the tech support number for Microsoft. The caller dialed the number for assistance and scammers were able to steal thousands of dollars from her.

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 the FTC (1-877-382-4357) or local law enforcement. You can also file a complaint online at **reportfraud.ftc.gov**.

MORE INFORMATION

- For more details about tech support scams, the Better Business Bureau has useful information at **www.bbb.org/article/news-releases/16553-bbb-tip-tech-support-scams**.
- The FTC provides additional information on how to spot and avoid tech support scams at **consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams**.

Government Imposter Scams

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, demand payment for "taxes" or "fees," or allege some problem in order to steal your money or personal information. They may also use documents or images, like a federal logo, when communicating with the intended victim to make their claim seem legitimate. Among the different types of government imposter scams, Social Security-related ones were the most common scam of this type reported to both the Committee's Fraud Hotline and the FTC in 2023. According to the FTC, victims lost over $126 million to Social Security imposter scams last year.[21]

Reports from the Fraud Hotline

A caller from West Virginia reported that he received a call from a scammer who claimed to be an employee of the federal government. The caller said he was told to send $900 to the scammer to erase his debt with the IRS.

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 the FTC (1-877-382-4357) or local law enforcement. You can also file a complaint online at **reportfraud.ftc.gov**.

MORE INFORMATION

- The FTC provides tips on how to spot and avoid imposter scams at **consumer.ftc.gov/features/imposter-scams**.
- SSA has more information on how to protect yourself from Social Security Scams at **www.ssa.gov/scam**.

Romance Scams

Romance scammers exploit an individual's desire for companionship and love by creating fake identities and forming emotional connections online. These scammers often pose as potential romantic partners, gaining victims' trust over time through frequent communication and declarations of affection. Once trust is established, the scammer typically fabricates a crisis or urgent need for money, such as medical expenses, travel costs, or investments, persuading the victim to send funds. Victims may be manipulated into keeping the relationship secret or rushed into making financial transactions before fully verifying the authenticity of their supposed partner.

Romance scams are pervasive across dating websites, social media platforms, messaging apps, and online forums. Awareness and caution are crucial in recognizing the signs of deception and protecting oneself from emotional and financial harm. The FTC reports that more than 64,000 consumers reported they were victims of romance scams in 2023, with reported losses totaling over $1.1 billion.[22]

Reports from the Fraud Hotline

A woman from Ohio called the Fraud Hotline to report that, for the past two years, she has been the victim of a romance scam where she lost $40,000.

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, P2P payment app, or gift card.

STEPS TO PREVENT AND RESPOND

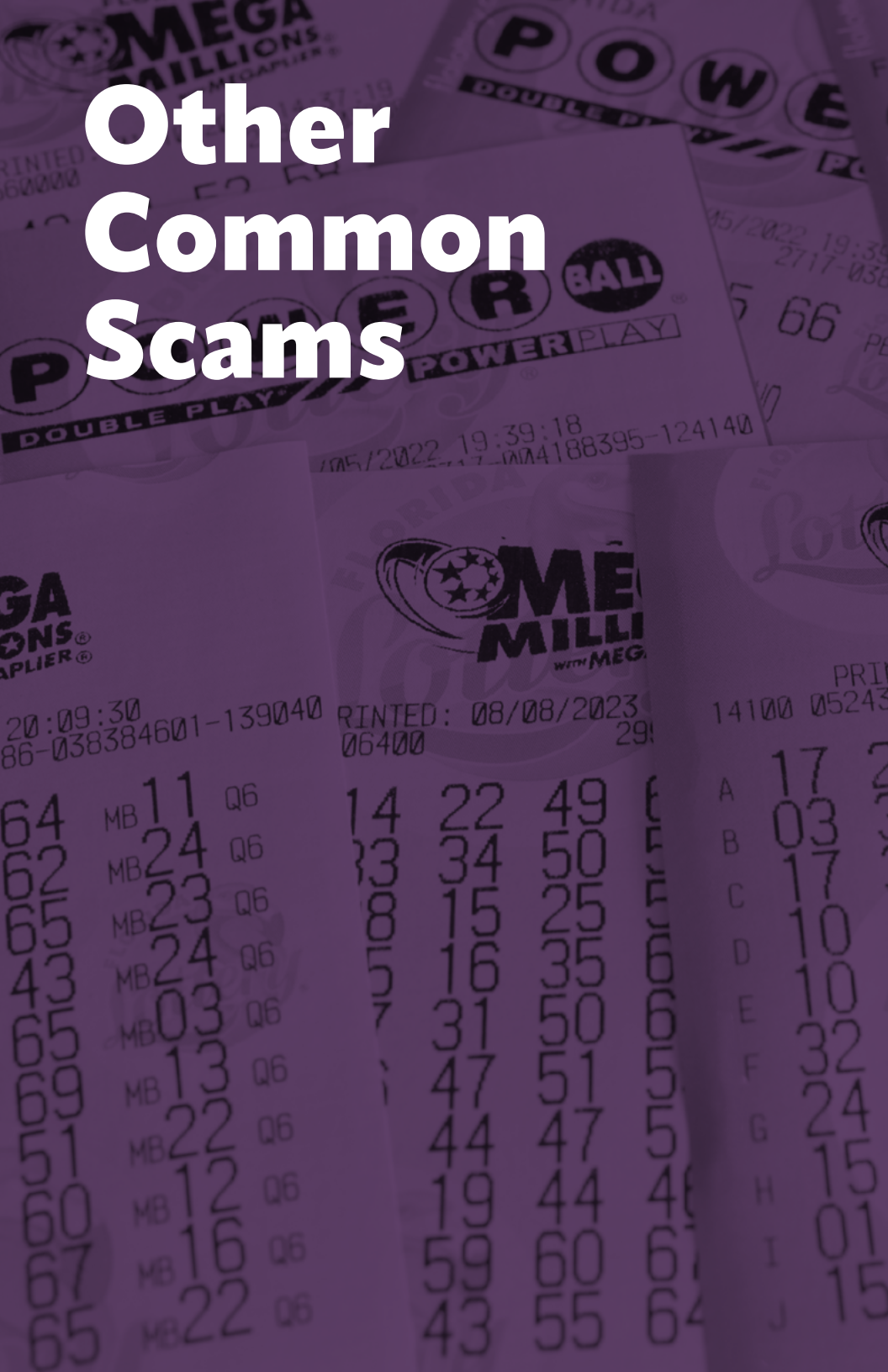
- If the person always refuses to video call or meet in person, block them.
- Never send money or gifts to someone that you have not met in person.

- 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 the FTC (1-877-382-4357) or local law enforcement. You can also file a complaint online at **reportfraud.ftc.gov**.

MORE INFORMATION

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

Other Common Scams



Sweepstakes & Lottery Scams

Sweepstakes and lottery scams exploit individuals' hopes of winning a large cash prize by deceiving them into believing they have won a contest they never entered. Scammers often contact victims via text message, phone, email, or mail, claiming they have won a substantial sum but need to pay "taxes" or "fees" upfront to claim the prize. These fraudulent schemes manipulate the excitement and desire for financial gain, urging victims to provide personal information or send money, only to disappear once the payment is made. Awareness and caution are crucial to avoid falling victim to these deceptive practices, as once money is sent, it is typically irretrievable, leaving victims financially and emotionally devastated. In 2023, the FTC found that victims reported $338 million in losses to prize, sweepstakes, and lottery related scams.[23]

Reports from the Fraud Hotline

A woman from Pennsylvania reported that she was contacted by a scammer who claimed she had won the lottery. The scammer told the woman that in order to claim the prize, she had to pay $800.

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 the FTC (1-877-382-4357) or local law enforcement. You can also file a complaint online at **reportfraud.ftc.gov**.

MORE INFORMATION

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

Investment Scams and Other "Get Rich Quick" Schemes

Through investment scams, fraudsters will boast about the possibility of high returns with little effort and little risk from you, if you invest in a new opportunity, like cryptocurrency, real estate, or precious metals. Investment scams may start on social media, online dating apps, or from unsolicited contact through a text message, phone call, or email. They often begin with the scammer building a relationship with their intended victim. Once the scammer has the victim's trust, they will then encourage them to invest, while guaranteeing risk-free, high returns. According to the FBI's IC3, in 2023, investment scams were the costliest scams for older adults, with reported losses topping $1.2 billion.[24] Losses incurred by older adults from investment scams have increased by more than 400 percent since 2021.[25]

Reports from the Fraud Hotline

A caller from Pennsylvania reported that he cashed out his 401K and deposited all of his funds into what he thought was a high yield savings account. The caller reported that the website for the fake investment company has since vanished, and he has been unable to withdraw any of his money, leaving him without any retirement funds.

BEWARE: PYRAMID SCHEMES

Pyramid schemes are also a type of investment scam. Pyramid schemes pose as real job opportunities but function on a deceptive model where participants are enticed with the promise of high returns for recruiting others, rather than selling genuine products or services. Often, participants are required to invest upfront, believing they will earn substantial profits. Pyramid schemes rely on continuous recruitment by participants, where participants persuade friends and acquaintances to join. While early participants may receive payouts from fees paid by newer recruits, pyramid schemes are unsustainable and inevitably collapse, leaving the majority of participants with financial losses. These schemes exploit people's desire for quick wealth, offering false hopes of financial success without legitimate income opportunities. Authorities globally

classify pyramid schemes as fraudulent and warn against involvement to prevent financial hardship and legal consequences.

BEWARE: CONFIDENCE INVESTMENT SCAMS

Confidence investment scams, also referred to as "pig butchering scams," involve fraudsters cultivating a fake online relationship with their victims to gain trust and convince them to invest in what they think is a sound investment opportunity but is actually a fraudulent scheme. The term "pig butchering" was coined by the scammers themselves and refers to the practice of "fattening up" the victim with affection and attention before "butchering" them financially. Scammers often pose as potential romantic partners or new friends, and convince their targets to invest in fake cryptocurrency platforms, or other fake financial opportunities. Once the victim invests money, the scammer disappears with the funds, leaving the victim not only financially devastated but also emotionally betrayed. This scam has been increasingly prevalent in recent years, taking advantage of the growing popularity of online dating and social media platforms.

RED FLAGS

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

- The scammer promises high, short-term profits or returns with little effort.
- They pressure you to act quickly by telling you that you could lose your chance to win big.
- The scammer claims there is little risk to the investment and guaranteed returns. This is a scam. All investments come with the risk that you may lose money.
- They give few details about the investment. Fraudsters usually fail to provide a brochure or other written information detailing the scope or risks of the investment.
- They promise a secret, proven system that will allow you to make lots of money quickly and with little effort.
- They require you to pay an upfront fee, buy starter kits, or invest in products or services before you can start earning money. Legitimate jobs typically do not require you to pay to work.
- Pyramid schemes emphasize recruiting others into the scheme rather than selling genuine products or services to customers. If the primary focus is on recruiting new members and earning commission from their investments or memberships, it's likely a pyramid scheme.

STEPS TO PREVENT AND RESPOND

- Do not invest money based on advice from someone you have solely met online or through an app.
- Beware of unsolicited offers. Always be skeptical of unsolicited calls, text messages, emails, or social media messages.
- Do not rush to invest. If this is a legitimate investment, it will continue to be available.
- Check credentials and independently verify any information you are provided or statements you are shown. Most investment scams involve unregistered actors.
- Know your finances. If you cannot afford to lose some or all of your investment, you should think twice about investing.
- Consult with a financial advisor or trusted family member or friend if you have doubts.
- Report all suspicious calls or messages to the FTC (1-877-382-4357) or local law enforcement. You can also file a complaint online at **reportfraud.ftc.gov**.
- File a complaint with the U.S. Securities and Exchange Commission (SEC) at **sec.gov/tcr**.

MORE INFORMATION

- Check SEC's EDGAR database to check the veracity of the claims at **www.sec.gov/edgar/search-and-access**.
- If you have an investment problem or question, your state securities regulator may be able to help you. To find a regulator in your state, visit **www.nasaa.org/contact-your-regulator** or call 202-737-0900.
- The FTC has more information about scams that involve money-making opportunities and investments at **consumer.ftc.gov/jobs-and-making-money/money-making-opportunities-and-investments**.

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. There were $17 million in confirmed losses due to health care scams in 2023, but the actual number is estimated to be much higher since these losses are more likely to go unreported.[26]

Reports from the Fraud Hotline

A caller from Massachusetts was contacted by a scammer purporting to be a Medicare employee. The scammer said the caller's Medicare card was expiring and requested the caller's Medicare number and his doctor's name.

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. The government will never charge you for a new or replacement Medicare card.
- You receive a call from someone who says your Medicare card is expiring. This is a scam. As long as you remain enrolled in Medicare and pay your monthly premium, your Medicare card will not expire.
- 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 **www.healthcare.gov/find-assistance/** directly for help. Those eligible for Medicare can find assistance with their State Health Insurance Assistance Programs (SHIPs) at **www.shiphelp.org/**.
- Report all suspicious calls or messages to the FTC (1-877-382-4357) or local law enforcement. You can also file a complaint online at **reportfraud.ftc.gov**.

MORE INFORMATION

- The FTC provides additional information and tips at **consumer.ftc.gov/articles/spot-health-insurance-scams**.
- The FCC has more information on Medicare scams at **fcc.gov/older-americans-and-medicare-scams**.
- The Centers for Medicare & Medicaid Services (CMS) has resources for reporting scams or attempted scams at **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 **oig.hhs.gov/fraud/consumer-alerts**.

Travel, Vacations, and Timeshare Scams

Travel, vacation, and timeshare scams exploit people's desire for affordable luxury and relaxation. These scams typically begin with enticing offers of free trips, heavily discounted vacation packages, or exclusive timeshare deals, often delivered through unsolicited phone calls, emails, or flashy online ads. The scammers persuade victims to pay upfront fees for booking, taxes, or membership, promising incredible value that doesn't materialize.

In the case of timeshare plans, the deception can be even more insidious. Fraudsters use high-pressure sales tactics to push individuals into purchasing vacation properties, often under false pretenses or with misleading terms. Once locked into a timeshare contract, victims frequently find that escaping the agreement is nearly impossible, facing ongoing maintenance fees, special assessments, and a lack of resale market. The supposed benefits of timeshare ownership, such as flexibility and cost savings, often evaporate, leaving owners with significant financial burden and no easy way out. This can turn what was meant to be a dream vacation into a long-term financial nightmare. The FTC reported more than $122 million in losses due to vacation and timeshare scams.[27]

Reports from the Fraud Hotline

A woman in Florida called the Hotline and explained that she was promised a timeshare plan with zero percent financing. She has been unable to use her plan and has been left with extensive hidden fees. She has been unable to cancel her timeshare plan.

RED FLAGS

Vacation and timeshare scammers will often employ these tactics:

- Be cautious of unexpected offers or aggressive sales tactics that push you to make quick decisions without adequate research.
- Avoid deals requiring upfront payments for taxes, booking, or memberships to claim "free" or heavily discounted vacations. Legitimate offers typically don't ask for such fees in advance.
- Watch out for vague, unclear, or overly complex contracts that obscure the true costs and conditions of timeshare deals. Always review contracts carefully and seek professional advice if needed.

STEPS TO PREVENT AND RESPOND

- Verify the legitimacy of the company and the offer by checking reviews, ratings, and regulatory status.

- Avoid offers requiring upfront fees for taxes, booking, or memberships, especially for "free" or heavily discounted deals.
- Review all terms and conditions in detail, and consider consulting a legal or financial advisor before signing any contract.
- If you feel rushed or pressured into making a decision, take a step back and reconsider. Legitimate offers will provide ample time for you to think things through.
- Report any suspicious calls, emails, or mailers to the FTC (1-877-382-4357) or local law enforcement. You can also file a complaint online at **reportfraud.ftc.gov**.

MORE INFORMATION

- The FTC has more information on travel, vacation, and timeshare scams at **consumer.ftc.gov/articles/timeshares-vacation-clubs-and-related-scams**.

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 2023, the FTC reported over one million cases of identity theft,[28] and an AARP report found that Americans lost $43 billion due to identity theft that same year.[29]

Reports from the Fraud Hotline

A Delaware man received a call from someone attempting to steal his personal identifying information by posing as an employee of the state energy company.

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

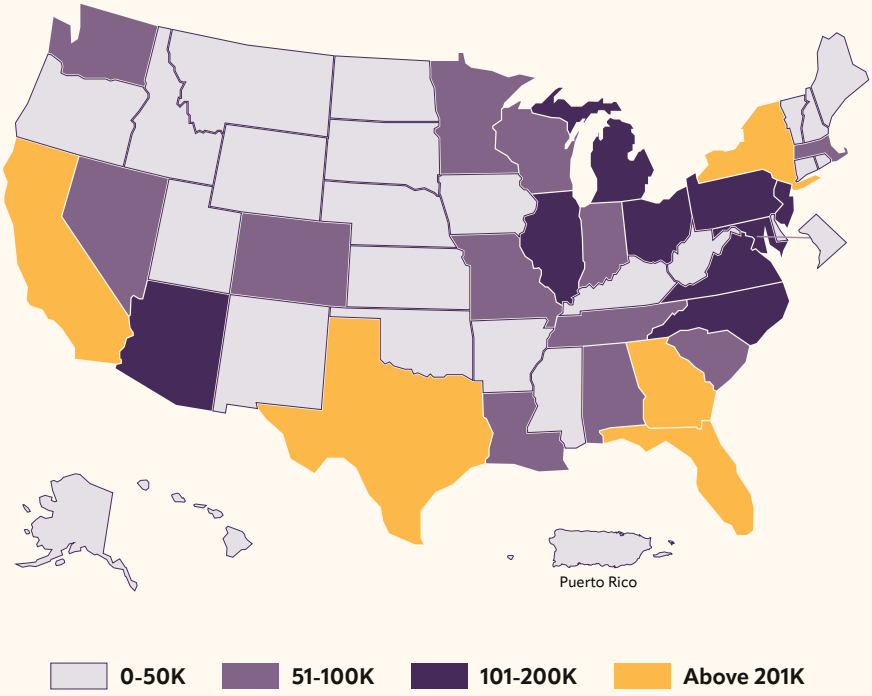
- If someone asks you for your Social Security Number or personal information on the phone, hang up. If they claim to be from a legitimate company or agency, go to that organization's official website and call their official line to verify.
- Do not click on email links or open attachments, even if the 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 the FTC (1-877-382-4357) or local law enforcement. You can also file a complaint online at **reportfraud.ftc.gov**.

MORE INFORMATION

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

NUMBER OF COMPLAINTS REPORTED TO FTC IN 2023, BY STATE:



State	2023
Alabama	68,818
Alaska	7,502
Arizona	107,477
Arkansas	30,171
California	537,766
Colorado	76,736
Connecticut	48,949
Delaware	18,673
District of Columbia	16,687

State	2023
Florida	435,579
Georgia	219,245
Hawaii	14,101
Idaho	17,198
Illinois	185,133
Indiana	71,890
Iowa	25,126
Kansas	27,452
Kentucky	40,221
Louisiana	63,121
Maine	13,317
Maryland	105,309
Massachusetts	89,545
Michigan	121,894
Minnesota	54,493
Mississippi	34,168
Missouri	73,176
Montana	10,120
Nebraska	18,252
Nevada	60,535
New Hampshire	15,022
New Jersey	131,480
New Mexico	21,541
New York	267,377
North Carolina	145,904
North Dakota	5,764

State	2023
Ohio	146,405
Oklahoma	38,046
Oregon	50,988
Pennsylvania	194,291
Rhode Island	11,906
South Carolina	76,116
South Dakota	6,274
Tennessee	88,131
Texas	437,790
Utah	32,499
Vermont	6,188
Virginia	120,307
Washington	92,478
West Virginia	16,233
Wisconsin	56,339
Wyoming	5,286
Puerto Rico	7,533
Unknown*	957,971
All Areas	**5,524,523**

Note: The number represents total fraud, identify theft, and other reports to FTC's Consumer Sentinel Network, instead of a statistically representative measure of the incidence of scams or financial exploitation of older adults in each state. Calls are likely reflective of consumer awareness of FTC and its partners.
*Unknown represents the reports not labeled under the 50 states, District of Columbia, or Puerto Rico.

Resources

ADDITIONAL TIPS ON HOW TO PROTECT YOURSELF FROM SCAMMERS WHO MAY ATTEMPT TO CONTACT YOU THROUGH THE FOLLOWING MECHANISMS:

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. Scammers may also pretend to contact you accidentally through a fake wrong-number text message scam. In this scam, you may receive a text message purportedly intended for someone else or from someone who purports to know you. Recipients of "wrong-number" text messages often respond out of politeness or curiosity. The scammer then uses that initial response to build a connection, which makes you more suspectable to scams like a romance scam or cryptocurrency investment scam.

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.
- If you receive a text that you think could be a scam, block the number so they are unable to contact you again. Do not respond because if you do, it could lead to more texts from scammers.

- 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 copying the message and forwarding it to 7726 (SPAM). This can help your cell phone provider identify and block similar spam messages.

Online Ads and Pop-ups: 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.

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

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.
- Be cautious of any ads you see on social media – it could be a scam.
- 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 platforms are one of the most common contact methods used by scammers targeting older adults online and offer scammers an opportunity to access personal details and gain the trust of the target.

According to the FTC, for the third year in a row, victims lost more money to scams that originated on social media than through any other contact method. In 2023, there was a reported $1.4 billion in losses to scams that started through social media platforms, primarily through Facebook and Instagram. The largest reported losses to scams perpetuated through social media were from investment scams.[30]

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.
- If you receive an urgent online request for money or an investment from a friend or contact on social media, it is most likely a scam. If you think it could be genuine, confirm with them on another platform or meet them in person to verify. **Be aware:** their account may have been hacked, especially if they ask you to send cryptocurrency, gift cards, or a bank transfer.
- Watch out for fake ads on social media. Before you buy something through an ad on social media, verify the company. Search online for its name plus "scam" or "complaint."

Phone Calls: Unwanted calls and robocalls are the top complaints that the FCC receives.[31] 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.

- 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.
- 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 the FCC at 1-888-225-5322 or the FTC at 1-877-382-4357 as soon as possible. You can also file a complaint online at reportfraud.ftc.gov.

Email: Scammers often use phishing emails to trick individuals into giving away their personal information. Here are examples of emails you might receive that are most likely scams:

- An email claims you need to verify or update your account information, directing you to a fake login page.
    - ◊ **Do not** put your information in this page. Scammers are able to capture your username and password and login to the real site using your account.
- An email warns of suspicious activity on your account and urges you to click a link to secure it.
    - ◊ **Do not** click on links or download attachments from unknown or suspicious emails.
- An email informs you that you have won a prize or reward but must provide personal information or pay a fee to claim it.
- An email creates a sense of urgency, stating that your account will be locked unless you provide sensitive information immediately.
- An email contains an unexpected invoice or receipt and prompts you to open an attachment or click a link to review it.

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

You can also 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 www.house.gov. To locate your Senator, go to 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.

Service	Resource	Website	Phone
Victim Support and Counseling	VictimConnect Resource Center	victimconnect.org/get-help/	1-855-484-2846
Legal Help	Legal Services Corporation	www.lsc.gov/about-lsc/what-legal-aid/get-legal-help	Use the search tool to find the phone number for the local legal aid office
Other Services	Eldercare Locator	eldercare.acl.gov/	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) 808-5318
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
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

State/Territory	Phone Number
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
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: **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 provides information for older Americans and their family members on how to report fraud 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 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), Consumer Sentinel Network Data Book 2023, pg 11, **https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf** (last visited August 13, 2024)

2 FTC, "Think you know what the top scam of 2023 was? Take a guess," **https://consumer.ftc.gov/consumer-alerts/2024/02/think-you-know-what-top-scam-2023-was-take-guess** (last visited August 13, 2024)

3 Aging Committee Hearing, "Modern Scams: How Scammers Are Using Artificial Intelligence & How We Can Fight Back," **https://www.aging.senate.gov/hearings/modern-scams-how-scammers-are-using-artificial-intelligence-and-how-we-can-fight-back** (last visited August 13, 2024)

4 National Adult Protective Services Association (NAPSA), "Learning About Financial Exploitation," **https://www.napsa-now.org/financial-exploitation/** (last visited August 13, 2024)

5 U.S. Department of Treasury Financial Crimes Enforcement Network (FinCEN), "Financial Institutions Report $27 Billion in Elder Financial Exploitation Suspicious Activity in One-Year Period," **https://www.fincen.gov/news/news-releases/fincen-issues-analysis-elder-financial-exploitation** (last visited August 13, 2024)

6 AARP, The Scope of Elder Financial Exploitation: What It Costs Victims, pg 1, https://www.aarp.org/content/dam/aarp/money/scams-and-fraud/2023/true-cost-elder-financial-exploitation.doi.10.26419-2Fppi.00194.001.pdf (last visited August 13, 2024)

7 FinCEN, Advisory on Elder Financial Exploitation, pg 2, https://www.fincen.gov/sites/default/files/advisory/2022-06-15/FinCEN%20Advisory%20Elder%20Financial%20Exploitation%20FINAL%20508.pdf (last visited August 13, 2024)

8 Federal Bureau of Investigation (FBI), Elder Fraud Report 2023, pg 10, https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3ElderFraudReport.pdf (last visited August 13, 2024)

9 FBI, Elder Fraud Report 2023, pg 16-17, https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3ElderFraudReport.pdf (last visited August 13, 2024)

10 FTC, Consumer Sentinel Network, All Fraud Reports by Payment Method, https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods (last visited August 13, 2024)

11 Analysis of FTC data by Aging Committee staff. The analysis compares 2023 data to 2022 data. FTC data is available online at: https://public.tableau.

com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods (last visited on August 13, 2024)

12 FTC, Consumer Sentinel Network, All Fraud Reports by Payment Method, https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods (last visited August 13, 2024)

13 FTC, Consumer Sentinel Network Data Book 2023, pg 5, https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf (last visited August 15, 2024)

14 FTC, Consumer Sentinel Network Data Book 2023, pg 7, https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf (last visited August 15, 2024)

15 FTC, Consumer Sentinel Network, Imposter Scams in 2023, https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts (last visited August 16, 2024)

16 FBI, "FBI Warns of Scammers Targeting Senior Citizens in Grandparent Scams and Demanding Funds by Wire, Mail, or Couriers," https://www.ic3.gov/Media/Y2023/PSA231117 (last visited August 15, 2024)

17 FTC, Consumer Sentinel Network Data Book 2023, pg 7, https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf (last visited August 15, 2024)

18 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 August 16, 2024)

19 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 August 16, 2024)

20 FBI, Elder Fraud Report 2023, pg 7-8, https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3ElderFraudReport.pdf (last visited August 15, 2024)

21 FTC, "Explore Government Imposter Scams," https://public.tableau.com/app/profile/federal.trade.commission/viz/GovernmentImposter/Infographic (last visited August 16, 2024)

22 FTC, "'Love Stinks' – when a scammer is involved," https://www.ftc.gov/business-guidance/blog/2024/02/love-stinks-when-scammer-involved (last visited August 15, 2024)

23 FTC, Consumer Sentinel Network Data Book 2023, pg 8, https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf (last visited August 15, 2024)

24 FBI, Elder Fraud Report 2023, pg 3, 15, https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3ElderFraudReport.pdf (last visited August 15, 2024)

25 FBI, "FBI Highlights Growing Number of Reported Elder Fraud Cases Ahead of World Elder Abuse Awareness Day," https://www.fbi.gov/news/press-releases/fbi-highlights-growing-number-of-reported-elder-fraud-cases-ahead-of-world-elder-abuse-awareness-day (last visited August 15, 2024)

26 FTC, Consumer Sentinel Network Data Book 2023, pg 8, https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf (last visited August 15, 2024)

27 Id.

28 Id.

29 AARP, "Identity Fraud Cost Americans $43 Billion in 2023," https://www.aarp.org/money/scams-fraud/info-2024/identity-fraud-report.html (last visited August 15, 2024)

30 FTC, "Who's who in scams: a spring roundup," **https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2024/05/whos-who-scams-spring-roundup** (last visited August 15, 2024)

31 Federal Communications Commission (FCC), "Stop Unwanted Robocalls and Texts," **https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts** (last visited August 15, 2024)

Notes

Notes

Notes

Notes

Fraud Hotline

1-855-303-9470

U.S. Senate
Special Committee on Aging