

Fighting Fraud:

Top Scams in 2021

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

Senator Tim Scott (R-SC),
Ranking Member



U.S. Senate
Special Committee on Aging

TABLE OF CONTENTS

About the Senate Special Committee on Aging	4
How Scammers are Stealing People's Money	8
Top 10 Scams in 2021	13
1. Government Imposter Scams	15
2. Identity Theft	18
3. Business Impersonation & Shopping Scams	21
4. Robocalls & Unsolicited Calls	24
5. Health Care & Health Insurance Scams	27
6. Sweepstake & Lottery Scams	30
7. Tech Support & Computer Scams	33
8. Romance Scams	37
9. Financial Services Impersonation & Fraud	40
10. Person-In-Need & Grandparent Scams	44
Scams by State	46
Resources	50
Endnotes	62

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
JACKY ROSEN, Nevada
MARK KELLY, Arizona
RAPHAEL G. WARNOCK, Georgia

TIM SCOTT, South Carolina, RANKING MEMBER

SUSAN M. COLLINS, Maine
RICHARD BURR, North Carolina
MARCO RUBIO, Florida
MIKE BRAUN, Indiana
RICK SCOTT, Florida
MIKE S. LEE, Utah

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

MESSAGE FROM CHAIRMAN CASEY AND RANKING MEMBER SCOTT

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 at 1-855-303-9470, Monday through Friday, 9 AM to 5 PM Eastern Time. The Committee staff who operate the Fraud Hotline provide callers with information to report incidences of fraud to the proper officials, such as law enforcement and government agencies. In 2021, more than 650 individuals from across the country contacted the Committee's Fraud Hotline.

In 2021, the top 10 scam types reported to the Committee shared many similarities with the data reported by the Federal Trade Commission (FTC), with imposter scams ranking as the most reported category for both. Monetary losses due to scams continue to rise; in 2021, consumers reported more than \$5.8 billion in losses to the FTC, an increase of more than 70 percent over the previous year. Older adults report the highest losses per person.¹

In October 2021, the Committee held a hearing entitled, "Frauds, Scams and COVID-19: How Con Artists Have Targeted Older Americans During the Pandemic." Witnesses testified to the ways in which the pandemic exacerbated risks for older adults and led to a rise in romance scams, where bad actors play towards their targets' emotional susceptibility to gain trust. The FTC

reports that people ages 70 and older have the highest median losses to romance scams, totaling \$9,000 each.²

The Committee continues its work to educate and raise awareness of fraud risks targeting older adults. In addition to the Committee's annual Fraud Book, in 2021, Spanish versions of the Fraud Book and fraud prevention resources were released, which can be found on the Committee's website: www.aging.senate.gov.

In February 2022, the bipartisan Stop Senior Scams Act (S. 337) was signed into law. This legislation was drafted as a result of the Committee's work and directs the FTC to create a Federal Advisory Council charged with bringing together government officials, industry representatives, advocates, and consumers to develop model educational materials for retailers and financial institutions to stop scams targeting seniors.

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 look forward to building upon our successful efforts to stop scams that target our Nation's seniors.

Sincerely,



Robert P. Casey, Jr.
Chairman



Tim Scott
Ranking Member

How scammers are stealing people's money

To steal people's money, scammers rely on contact methods that allow 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.

SPOTLIGHT ON CONTACT METHODS: PHONE & SOCIAL MEDIA

Phone: In 2021, phone calls were the main method of contact used by scammers to reach older adults, according to the FTC.³ One out of four Americans over the age of 60 were contacted by scammers via phone.⁴ FTC data also shows that the phone is the most common method used by scammers to contact the oldest segment of the population, those ages 80 and older.⁵ Scammers can use phone calls to impersonate government agencies or family members, sometimes masking their caller ID as the person or agency they are impersonating, a tactic known as "spoofing."

Tips to protect yourself:

- Do not answer calls from unknown numbers. If you answer such a call, hang up immediately.
- You may not be able to tell right away if an incoming call is real or not. Be aware: Caller ID showing a "local" number does not necessarily mean it is a local caller.
- Do not respond to any questions asked by a stranger on a call.
- If you answer the phone and the caller – or a recording – asks you to hit a button to stop getting the calls, you should just hang up. Scammers often use this trick to identify potential targets.

Social Media: According to the FTC data, the percentage of older adults who lost money and were contacted by scammers using social media increased from 3 percent in 2017 to 15 percent in 2021.⁶ FTC data also show older adults ages 60 to 69 are more likely to be contacted using social media than those ages 80 and older.⁷ As older adults become more active online, scammers may increasingly use social media as a method of contact. Social media offers scammers an opportunity to access personal details and gain trust from the older adult.

Tips to protect yourself:

- Do not accept a new friend request from someone that you already have as a friend or that normally is not connected on 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, win a gift card, take a quiz, fill out a survey, or watch a video.
- Avoid clicking on ads that offer low prices on popular items and brands.
- Avoid quizzes and other similar social media threads that ask you to provide personal information, such as places you have visited, your favorite food, hobbies, or pets.
- Stop all contact with a potential scammer by blocking instant messages and email addresses.
- Protect your social media account access by using strong passwords and privacy settings to hide information like your city, phone number, and date of birth.

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

Gift Cards: In 2021, 27 percent of older adults ages 60 and older paid a scammer using a gift card or a reloadable card, according to the FTC.⁸ Gift cards were the main payment method used by scammers to request and steal money from older adults.⁹ When the older person sends the card number, a scammer immediately uses the balance, making it difficult 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 key signs of scams, like requests to buy cards at several stores or to purchase a specific type of card.

Peer-to-Peer Payments: According to FTC data, scammers' requests of payments from older adults via money-transfer payment apps increased from 2 percent in 2017 to 10 percent in 2021.¹⁰ These peer-

to-peer (P2P) payment methods are often abused by scammers because they get the money instantly and anywhere and do not allow for a transaction to be cancelled once sent.

Tips to protect yourself:

- Avoid sending money to anyone you do not know. Take your time to be sure that you are sending money to the right person.
- Set up fraud alerts in your P2P app or with the bank or credit card account that you linked to the app. Fraud alerts can let you know if personal information has been changed or transactions have been made.
- P2P payments have social media elements, like lists of friends. Avoid sharing information like your address, phone number, and other personal details and ignore friend requests from people you do not know.
- Like any other financial website, protect your account with a strong password. Use two-factor authentication, which requires you to enter a numeric code given in an email or text in addition to your username and password.
- If you suspect you have been a victim, contact your P2P company and your bank and credit card company as soon as possible. They may be able to put a hold on the transaction. You may have some protections if you did not authorize the transaction.

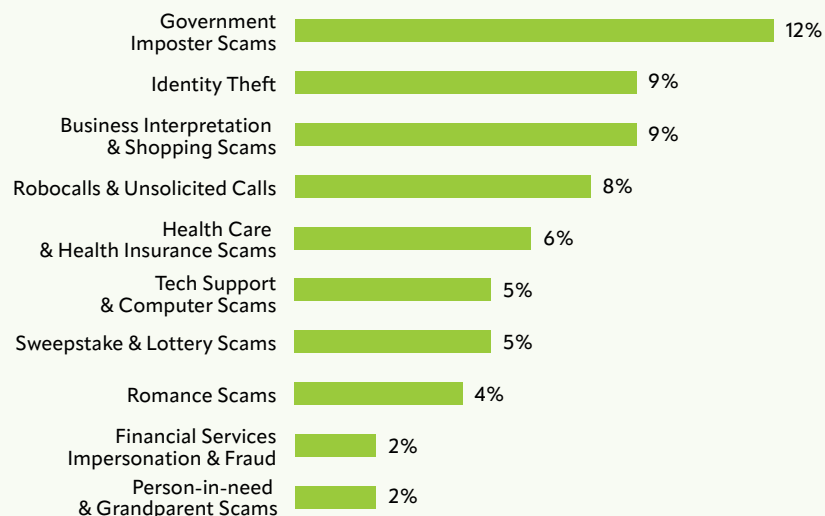
Top 10 Scams in 2021

In 2021, the Committee's Fraud Hotline received 667 new complaints from residents across the country. These complaints bring the total number of complaints registered with the Fraud Hotline since 2015 to nearly 9,100.¹¹

Figure 1 shows the Top 10 scams in 2021. These scams account for 62 percent of complaints reported to the Committee's Fraud Hotline in 2021.

This book provides information to help older adults and their families respond to these Top 10 scams.

FIGURE 1: TOP 10 SCAMS IN 2021



Note: The percentages do not add up to 100 percent because categories that are not in the top 10 categories were excluded from this graph. In selecting the Top 10 categories, categories of calls that were not related to a specific type of scam or fraud (e.g. requests for referrals and information from the Fraud Hotline) or were broadly about a specific payment method, were excluded. Data for other categories can be found online at <https://www.aging.senate.gov/download/2021-fraud-book-additional-data>.



1. Government Imposter Scams

The top scam reported to the Committee's Fraud Hotline was the government imposter scam. In these fraudulent calls or emails, bad actors will pretend to be a representative of a federal agency, like the Social Security Administration (SSA) or Internal Revenue Service (IRS). They may threaten a person's benefits or demand they be sent money to "pay taxes or fees." In 2021, the most common scam of this type reported to the Fraud Hotline was Social Security fraud, with callers posing as representatives from SSA.

REPORTS FROM THE FRAUD HOTLINE

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 Social Security employee ID number, and the caller eventually hung up.

RED FLAGS

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

- You receive a phone call or email asking to confirm information that the government agency should already have, like an address or Social Security Number.
- The person calling or emailing 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.
- You are being pressured to make a decision 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.
- Never give out or confirm financial or other sensitive information unless you know who you are dealing with.
- 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.
- Spread the word: Spread the word: A government agency will never ask you to wire money, provide your Social Security number, or send funds via gift card.

- Call the number of the federal agency directly and wait to speak to a customer service representative to verify the call or email you received. Most likely, they will confirm that the call was a scam.
- If you do get a government imposter call, email, or mail, file a complaint with the FTC at [ftc.gov/complaint](https://www.ftc.gov/complaint).

MORE INFORMATION

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



2. Identity Theft

Identity theft scams are when a bad actor wrongfully obtains and uses another individual's personal data. Common targets for identity theft include 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 2020, the FTC took in nearly 1.4 million reports of identity theft.¹²

REPORTS FROM THE FRAUD HOTLINE

A woman in Illinois called the Fraud Hotline to report identity theft. The scammers pretended to be representatives from Medicaid and requested personal and financial information from the woman. They hacked into the woman's accounts, stole her Social Security number, bank account information, and passwords, and began using her identity to claim her benefits and cash out the money she had in her bank account.

RED FLAGS

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

- Someone reaches out to you in an unsolicited call or message and requests 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 inaccurate health conditions in your medical files.
- You do not receive your 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 or your computer at risk. If you want to visit the website in the email, do so manually in a separate search tab.

- Update your passwords to your accounts, especially if you suspect or learn that your bank or credit card company was breached. Do not use the same password for banks and credit card accounts.
- Subscribe to text and email alerts, especially those that inform you about unusual activity, like international, online, or large purchases.

MORE INFORMATION

- More information on identity theft can be found on the Department of Justice's 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>.



3. 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 provide fake phone numbers online that customers find when trying to seek assistance with a purchase. Scammers request personal or financial information from the individual to "resolve" the issue and instead gain access to their account. The FTC reports that these business impersonation scams disproportionately affect older adults.¹³

REPORTS FROM THE FRAUD HOTLINE

A woman in Maryland told the Fraud Hotline that she receives frequent calls from individuals claiming to be representatives of a major company. The callers tell her that she has several packages being shipped to her address even though she did not order them.

RED FLAGS

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

- When seeking assistance in 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 the real 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 by gift card nor will they need a picture of a gift card.

MORE INFORMATION

- The Small Business Administration (SBA) provides information and tips regarding business-related scams at <https://www.sba.gov/content/beware-scams>.
- The Federal Bureau of Investigation (FBI) shares information on scammers posing as legitimate businesses at <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise>.



4. Robocalls & Unsolicited Calls

Unwanted calls and robocalls are the top complaint that the Federal Communications Commission (FCC) receives¹⁴ and rank fourth 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 created by a prerecorded or robotic voice. Similarly, caller ID "spoofing" is when a caller disguises their phone number to appear to be local to the recipient or from a government agency in order to trick people into giving away personal information. The calls may also try to sell a product or service.

REPORTS FROM THE FRAUD HOTLINE

A woman from Maine called the Fraud Hotline to report two unsolicited calls she received. The calls referred her to an "agent" and claimed that if she did not speak with the agent, she would face legal ramifications.

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 button 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 phone number on your account statement or on the company's or government agency's website to verify the request, 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. If you answer such a call, hang up immediately.
- Do not respond to any questions, especially those that can be answered with "Yes."
- Never give out personal information, such as account numbers, Social Security Numbers, mother's maiden names, passwords, or other 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 and the FTC at 1-877-382-4357 as soon as possible.

MORE INFORMATION

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



Health care and insurance coverage decisions can be complex. Scammers take advantage of this complexity by impersonating Medicare or other health insurance providers or selling “discount health plans” that do not provide the coverage one needs. They may also request personal or financial information “in exchange for” benefits, vaccines, or other products related to the COVID-19 pandemic. The FCC finds that health-related scam calls tend to spike during Medicare’s open enrollment period, which runs from October to December.¹⁵

REPORTS FROM THE FRAUD HOTLINE

A woman from Pennsylvania received a call from a person claiming to represent the Centers for Medicare & Medicaid Services. The caller told her she needed a new Medicare card and requested she provide the location and name of her doctor’s office, her date of birth, and her Social Security number. They also asked about certain medical conditions and personal information in order to send her a “free kit.”

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 or email 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 that has little information or legitimate reviews online, and your doctor does not participate in it.
- You are given vague answers by a salesperson when you ask about specific details relating 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 a trusted source directly, like [Healthcare.gov](https://www.healthcare.gov) or [Medicare.gov](https://www.medicare.gov), to compare plans, coverage, and prices.

- Demand that you see a statement of benefits or a complete copy of the insurance policy that you are considering before making any decisions.
- Research any company offering health coverage, and if a 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/>.

MORE INFORMATION

- The FTC provides additional information and tips at <https://consumer.ftc.gov/articles/spot-health-insurance-scams>.
- The Centers for Medicare & Medicaid Services have resources for reporting scams or attempted scams at <https://www.medicare.gov/basics/reporting-medicare-fraud-and-abuse>.
- The Department of Health and Human Services maintains an extensive list of scam prevention information at <https://oig.hhs.gov/fraud/consumer-alerts/>.



6. Sweepstake & Lottery Scams

Sweepstakes scams 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. Criminals 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, electronic wire transfer, money order, or cash, in order to claim the prize. In 2020, the FTC found that older adults reported over \$69 million in losses to prize, sweepstakes, and lottery-related scams.

REPORTS FROM THE FRAUD HOTLINE

A caller from Delaware shared that her aunt was scammed when a bad actor called and told her that she had won \$7,000 and a sports car. In order to claim her prize, the scammer told her she needed to mail him \$3,500, which she did – but never received her supposed “winnings” in return.

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. Scammers will attempt to build a relationship with you.
- You are asked to pay the “tax” or “processing fee” by wiring money or sending money through the mail or via gift card.
- 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.
- Throw away letters saying you have won a prize if it mentions a “tax” or “fee” to claim.
- Report any suspicious calls, emails, or mailers to the FTC or your local law enforcement.

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>.



7. 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. 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 remote access to their computers and personal information. They may also request an individual's credit card or bank number so they can "bill" for their services to fix the virus. Another alternative to this scam is a pop-up window on a computer screen describing a security threat and instructing the user to contact a tech support agent. The FTC reports that older adults are likelier to lose money to tech support scams than younger people.¹⁶

REPORTS FROM THE FRAUD HOTLINE

An individual from Tennessee called the Fraud Hotline to report that she paid \$650 to get her computer fixed after having some technological issues. After giving control of her computer to the "tech employees," they instead accessed her bank account and maxed out a cash advance of \$20,000.

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 and that you must call a number to resolve the issue.
- A scammer says that the only solution to save your money from the “hacker” is to transfer your account funds to them while they get rid of the supposed virus, “protecting” your money.
- If you say that you would prefer to fix the issue by going to a physical store or calling a company yourself, a 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, go to the company website of the device on which you received the alert (e.g., Apple or Microsoft) and call their official tech support number.
- If a person calls you saying your device has been hacked or compromised by a virus, take down the number, hang up, and block the 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 or your local law enforcement.

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>.

KATE KLEINERT: ROMANCE SCAM SURVIVOR

Glenolden, Pennsylvania

"My husband, Bernie, passed away in 2009. Since then, I've never looked for any new romance in my life because I still feel married to my husband."

"But last summer, in August 2020, I received a friend request on Facebook... His name is Tony – well, that's what he told me."

"We started talking on the phone through an App he had me download. He told me he was a surgeon working in Iraq through a contract with the United Nations and that he has two children, a little boy and a girl. Tony became romantic much more quickly than I did and I kept trying to put him off, saying we didn't know each other. But Tony had the kids get in touch with me through email and they started calling me mom, which is my Achilles' heel..."

"Tony wanted to get married. He even asked if I wanted to go out and start looking at houses. I was constantly sending him gift cards, even though now I was using up the last of my husband's life insurance. My savings were gone... I kept doing this because he swore to me he would repay me the minute he got back to the States."

"I got a phone call from a man who said he was Tony's lawyer, who said that in Iraq, someone slipped drugs into Tony's bag and he knew nothing about it, but now he needed money for bail. He asked me for \$20,000. The lawyer told me to do whatever I could – put a mortgage on my house, borrow it from someone in my family. I couldn't do it."

"Even though this experience is painful to speak about, I want to be an ambassador to this experience because it's so devastating... In my case, I got pulled in because I had forgotten how good it felt to be loved."

Excerpts taken from Ms. Kleinert's testimony provided to the Committee in September 2021.



8. Romance Scams

Social media, dating sites, and other apps are all avenues that scammers use to develop false relationships and build trust, sometimes talking or messaging several times a day. These scammers target individuals seeking companionship and often quickly express their infatuation or love. The bad actor frequently "lives abroad." They may ask for money to pay for family issues, plane tickets, surgery or medical expenses, customs fees, or travel documents. Over the past 5 years, the FTC has reported people losing over \$1.3 billion to romance scams, more than any other FTC fraud category. In 2021, the average person reported roughly \$2,400 in losses.¹⁷

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 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.

MORE INFORMATION

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



9. Financial Services Impersonation & Fraud

In 2021, the most common financial services frauds reported to the Committee's Fraud Hotline were debt and mortgage fraud. In debt frauds, scammers impersonate debt collectors and try to trick their targets into paying a debt that does not exist. They may harass or threaten consumers with penalties or jail time. Mortgage relief scams may promise to make changes to a mortgage loan, lie about the terms of a loan, or guarantee services that they never deliver. According to the FTC, in 2021 nationally, there were over 151,000 reported cases of debt fraud and over 21,000 reported cases of mortgage fraud.¹⁸

REPORTS FROM THE FRAUD HOTLINE

A caller from Texas reported that a scammer impersonating a debt collector called to say that he owed student loans, even though he knew he had no student loan debt.

RED FLAGS

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

Debt Fraud

- The person calling you says you will go to jail if you don't pay. It is illegal for debt collectors to threaten to have someone arrested for not paying their debts.
- The person calling will not give you an answer about 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 calmly work with you. Scammers will pressure you to pay them while they have you on the phone.

Mortgage Fraud

- The person 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.
- In the documents you're being asked to sign, there are blank sections. 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

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 will object 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 are a scammer.
- Be sure to carefully read any documents before signing. If you have questions about something, ask the person attempting to get you to sign. If they brush aside your concerns, they are a scammer.

MORE INFORMATION

- The 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>.



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 claim that the grandchild is in trouble and needs money to help with an emergency, such as getting out of jail, paying a hospital bill, or leaving a foreign country. Scammers play on emotions and trick concerned family members into wiring them money. In July 2021, a federal indictment charged eight people who allegedly ran a national grandparent scam and stole an estimated \$2 million from more than 70 older adults between 2019 and 2020.

REPORTS FROM THE FRAUD HOTLINE

A South Carolina man called the Fraud Hotline to report that his father lost \$18,000 to a “grandparent scam” when a scammer came to his door and told him that his grandson was in jail after driving under the influence – when, in fact, his grandson was at work. The scammer said his grandson needed \$18,000 for bail to get out of jail, which the man paid.

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.

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.
- Check the story shared with trusted family and friends, even if you have been told to keep it a secret.

MORE INFORMATION

- To handle these calls, the FTC has helpful tips at <https://www.consumer.ftc.gov/articles/0204-family-emergency-scams>.

Scams by State

Scam

☐ Do not show this message again

Yes

No

KEY



Government Imposter Scams



Identity Theft



Business Impersonation & Shopping Scams



Robocalls & Unsolicited Calls



Health Care Scams



Sweepstake & Lottery Scams



Tech Support & Computer Scams



Romance Scams























Financial Services Impersonation & Fraud



Person-In-Need & Grandparent Scams

STATES WITH COMPLAINTS ABOUT THE
TOP 10 CATEGORIES OF SCAMS COVERED
IN THE FRAUD BOOK

State										
AK		•	•		•	•				
AL	•	•	•		•	•	•	•	•	•
AR	•	•	•	•	•	•	•	•	•	
AZ	•	•	•	•	•	•	•	•	•	•
CA	•	•	•	•	•	•	•	•	•	•
CO	•	•	•		•	•	•	•	•	•
CT	•		•	•	•	•	•	•	•	•
DE	•	•	•		•	•			•	•
FL	•	•	•	•	•	•	•	•	•	•
GA	•	•	•	•	•	•		•	•	
HI	•				•	•	•	•	•	
IA	•		•	•	•		•	•	•	
ID	•	•	•		•		•	•	•	
IL	•	•	•	•	•	•	•	•	•	•
IN	•	•	•		•	•	•	•	•	•
KS	•		•		•			•	•	•
KY	•		•		•	•	•	•	•	
LA	•	•	•		•	•		•	•	
MA	•	•	•	•	•	•	•	•	•	•
MD	•	•	•	•	•	•	•	•	•	•
ME	•	•	•	•	•	•	•	•	•	•
MI	•	•	•	•	•	•	•	•	•	•
MN	•		•	•	•	•	•	•	•	•
MO	•	•	•	•	•	•	•	•	•	
MS	•				•			•	•	

State										
MT	•		•							
NC	•	•	•	•	•	•	•	•	•	
ND			•		•					
NE	•		•		•	•		•	•	
NH	•	•	•	•	•	•				•
NJ	•	•	•	•	•	•		•	•	•
NM	•	•			•	•	•	•		•
NV	•				•	•		•	•	•
NY	•	•	•	•	•	•	•	•	•	•
OH	•	•	•	•	•	•		•	•	•
OK	•		•		•		•	•	•	•
OR	•	•	•		•	•	•	•	•	•
PA	•	•	•	•	•	•	•	•	•	•
RI	•		•		•			•	•	•
SC	•	•	•	•	•	•	•	•	•	
SD	•		•			•	•	•	•	
TN	•		•	•	•	•	•	•	•	•
TX	•	•	•	•	•	•	•	•	•	•
UT	•		•		•			•	•	
VA	•		•	•	•	•	•	•	•	•
VT	•					•				
WA	•	•	•	•	•	•	•	•	•	•
WI	•	•	•	•	•	•	•	•	•	•
WV	•	•	•		•	•		•		
WY	•				•		•	•		

Note: The types of scams reported by state are not a statistically representative measure of the prevalence of specific types of scams or financial exploitation of older adults in a given state. Calls to the Fraud Hotline reflect awareness of the Fraud Hotline among residents of a given state or jurisdiction.

Resources

ADDITIONAL RESOURCES FROM AGENCIES & OTHER ORGANIZATIONS

These organizations and websites provide information on a wide range of scams, including other common scams that target older adults and are not covered in this Fraud Book.

Entity	Website
Better Business Bureau (BBB)	https://www.bbb.org/scam-tracker
AARP Fraud Watch Network	www.aarp.org/fraudwatchnetwork
Federal Trade Commission (FTC)	https://consumer.ftc.gov/features/scam-alerts
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 victim. However, every year millions of older Americans are exploited by people known to them, whether it is 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.

GETTING HELP AFTER A SCAM

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

Service: Victim support and counseling

Resource: VictimConnect Resource Center

Website: <https://victimconnect.org/>

Phone: 1-855-484-2846

Service: 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

Service: 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	(800) 777-4590
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 them 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.

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 provide 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.

<input checked="" type="checkbox"/>	Important information to include in your complaint	Your notes
<input type="checkbox"/>	When did it happen?	
<input type="checkbox"/>	How were you contacted?	
<input type="checkbox"/>	What were you asked to do?	
<input type="checkbox"/>	How much money were you asked to provide?	

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

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

ENDNOTES

- 1 Federal Trade Commission (FTC), "New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021," <https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0> (last visited August 3, 2022)
- 2 FTC, "Reports of romance scams hit record highs in 2021," <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/02/reports-romance-scams-hit-record-highs-2021> (last visited August 3, 2022)
- 3 Analysis of FTC data by Aging Committee staff. The analysis combines total complaints for ages 60 to 69, 70 to 79, and 80 and older. FTC data is available online at: <https://public.tableau.com/app/profile/federal.trade.commission/viz/AgeandFraud/Infographic> (last visited August 3, 2022)
- 4 Analysis of FTC data by Aging Committee staff. The analysis combines total complaints for ages 60 to 69, 70 to 79, and 80 and older. FTC data is available online at: <https://public.tableau.com/app/profile/federal.trade.commission/viz/AgeandFraud/Infographic> (last visited August 3, 2022)
- 5 FTC, Explore Age & Fraud Loss, <https://public.tableau.com/app/profile/federal.trade.commission/viz/AgeandFraud/Infographic> (last visited August 3, 2022)
- 6 Analysis of FTC data by Aging Committee staff. The analysis combines total complaints for ages 60 to 69, 70 to 79, and 80 and older. FTC data is available online at: <https://public.tableau.com/app/profile/federal.trade.commission/viz/AgeandFraud/Infographic>
- 7 FTC, <https://public.tableau.com/app/profile/federal.trade.commission/viz/AgeandFraud/Infographic> (last visited August 3, 2022)
- 8 Analysis of FTC data by Aging Committee staff. The analysis combines total complaints for ages 60 to 69, 70 to 79, and 80 and older. FTC data is available online at: <https://public.tableau.com/app/profile/federal.trade.commission/viz/AgeandFraud/Infographic>
- 9 Analysis of FTC data by Aging Committee staff. The analysis combines total complaints for ages 60 to 69, 70 to 79, and 80 and older. FTC data is available online at: <https://public.tableau.com/app/profile/federal.trade.commission/viz/AgeandFraud/Infographic>

- 10 Analysis of FTC data by Aging Committee staff. The analysis combines total complaints for ages 60 to 69, 70 to 79, and 80 and older. FTC data is available online at: <https://public.tableau.com/app/profile/federal.trade.commission/viz/AgeandFraud/Infographic>
- 11 In addition, 2,057 complaints were submitted before 2015. The Aging Committee's Fraud Hotline was first launched in November 2013.
- 12 FTC, "New Data Shows FTC Received 2.2 Million Fraud Reports from Consumers in 2020," <https://www.ftc.gov/news-events/news/press-releases/2021/02/new-data-shows-ftc-received-22-million-fraud-reports-consumers-2020> (last visited August 3, 2022)
- 13 FTC, Protecting Older Consumers 2020–2021: A Report of the Federal Trade Commission, <https://www.ftc.gov/system/files/documents/reports/protecting-older-consumers-2020-2021-report-federal-trade-commission/protecting-older-consumers-report-508.pdf> (last visited August 3, 2022)
- 14 FCC, "Stop Unwanted Robocalls and Texts," <https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts>

- 15 FCC, "Health Care Scams Tend to Spike During Open Enrollment," <https://www.fcc.gov/health-care-scams-tend-spike-during-open-enrollment> (last visited August 3, 2022)
- 16 FTC, "Consumer Protection: Data Spotlight," https://www.ftc.gov/system/files/attachments/blog_posts/Older%20adults%20hardest%20hit%20by%20tech%20support%20scams/tech_support_spotlight_march2019.pdf (last visited August 3, 2022)
- 17 FTC, "FTC Data Show Romance Scams Hit Record High; \$547 Million Reported Lost in 2021," <https://www.ftc.gov/news-events/news/press-releases/2022/02/ftc-data-show-romance-scams-hit-record-high-547-million-reported-lost-2021> (last visited August 3, 2022)
- 18 FTC, "Consumer Sentinel Network 2021 Report," page 7, https://www.ftc.gov/system/files/ftc_gov/pdf/CSN%20Annual%20Data%20Book%202021%20Final%20PDF.pdf (last visited August 3, 2022)

Notes

Notes

Notes

Notes



U.S. Senate Special Committee on Aging