United States Senate
Special Committee on Aging

Fighting Fraud:

Senate Aging Committee Identifies

Top 5 Scams Targeting Our Nation's Seniors Since 2015

REMOVABLE POSTER INSIDE BACK COVER

Senator Robert P. Casey, Jr. (D-PA), Chairman
Senator Tim Scott (R-SC), Ranking Member

Tips from the United States Senate Special Committee on Aging for

Avoiding Scams

To convince you to give them money and personal information, scammers will often:

- Force you to make decisions fast and may threaten you.
- Use fake caller IDs to disguise their real numbers.
- Pretend to be a government employee (e.g. IRS or Social Security Administration).
- Pressure you not to consult with friends and family.
- Urge you to hand over personal information like your Social Security number or account numbers.
- Always remember: if an offer sounds too good to be true, it most likely is!

If you receive a suspicious call, hang up and please call the U.S. Senate Special Committee on Aging's Fraud Hotline at 1-855-303-9470

Table of Contents

Senate Special Committee on Aging

ROBERT P. CASEY, JR., Pennsylvania
CHAIRMAN

KIRSTEN GILLIBRAND, New York

RICHARD BLUMENTHAL, Connecticut

ELIZABETH WARREN, Massachusetts

JACKY ROSEN, Nevada

MARK KELLY, Arizona

RAPHAEL WARNOCK, Georgia

TIM SCOTT, South Carolina
RANKING MEMBER

SUSAN COLLINS, Maine

RICHARD BURR, North Carolina

MARCO RUBIO, Florida

MIKE BRAUN, Indiana

RICK SCOTT, Florida

MIKE LEE, Utah

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 coronavirus (COVID-19) pandemic has only exacerbated risks for seniors and made them even more vulnerable to scammers and schemes. In 2020, the Federal Trade Commission (FTC) estimates that seniors have lost $100 million to COVID-19-related fraud. The financial impact of fraud and scams on older Americans in normal times cannot be understated; however, the costs suffered throughout the pandemic are even more concerning. In 2020, the FTC estimated that Americans ages 60 and older lost at least $602 million to fraud, scams and financial exploitation schemes.

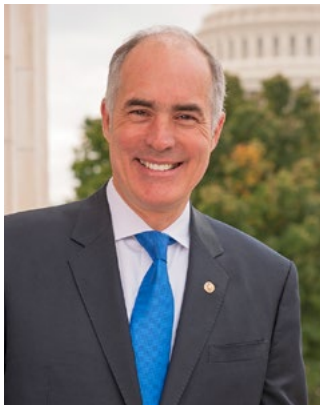
To combat fraud and scams, the Committee maintains a toll-free Fraud Hotline at 1-855-303-9470, Monday through Friday, 9 AM to 5 PM Eastern Time. Committee staff who operate the Fraud Hotline provide callers with information to report incidences of fraud to the proper officials, such as law enforcement and government agencies. In 2020, more than 600 individuals across the country contacted the Committee's Fraud Hotline. Since its inception in 2013, more than 10,000 individuals from all 50 states have contacted the Fraud Hotline to report fraud and scams.

To raise awareness of fraud and scams and increase reporting, the Committee compiles data from the calls it receives in an annual Fraud Book. This year, the Committee's Fraud Book includes information on other notable scams, including those perpetuated by the COVID-19 pandemic and romance scams, where a scammer poses as a "love interest" online and seeks to gain a victim's trust. The Fraud Book includes content on the top five most reported scams since 2015. These include: Government Imposter Scams, Sweepstakes Scams, Illegal Robocalls, Computer Scams and Grandparent Scams.

The Fraud Book also includes recommendations seniors can use to protect themselves against fraud, scams and financial exploitation. This section provides tips and resources for assistance in dealing with various fraudulent situations.

The Committee would like to thank the many consumer advocacy organizations, community centers and local law enforcement officials that provide invaluable assistance to consumers on these issues and encourage calls to the Fraud Hotline. We look forward to building upon our successful efforts to stop scams aimed at our nation's seniors.

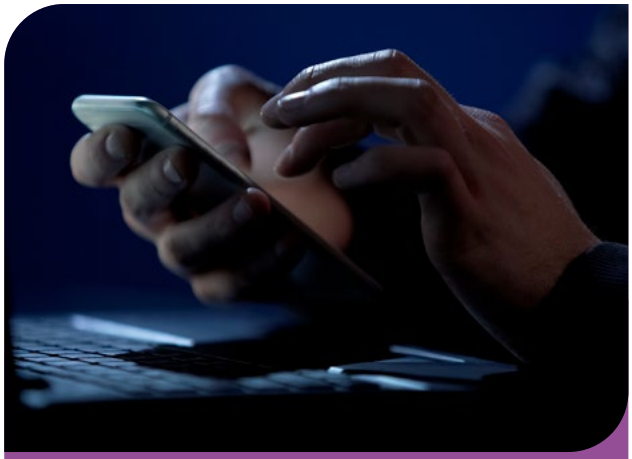
Sincerely,



Robert P. Casey, Jr.
Chairman

Tim Scott
Ranking Member

COVID-19 Scams



Fraud Case

A woman from San Francisco, California was so excited when she received a phone call informing her that she was now eligible to receive the COVID-19 vaccine. The caller informed her that she needed to answer some questions to book her appointment. After answering multiple questions, she became suspicious of the caller when he requested her Social Security Number. Once she realized she was getting scammed, the woman confronted the caller and he hung up the phone.

The emergence of COVID-19 has given scammers an opportunity to create and employ new tactics to steal money from seniors. COVID-19 scams target older Americans by employing these tactics to steal their money, including illegal robocalls, texts and emails and social media posts. Scammers use these means to make empty promises of COVID-19 miracle cures and means of preventions, or stimulus payments and incentives that are either unapproved or illegitimate.

The FTC and U.S. Food and Drug Administration (FDA) have sent warnings to companies that sell products such as herbal tea, essential oils, cannabinol and vitamin-C therapies, fraudulently claiming that they can cure or prevent COVID-19. The U.S. Federal Bureau of Investigation (FBI) reports that scammers are also advertising fake COVID-19 antibody tests in order to get personal information to use for identity theft and health insurance scams.

As of June 2021, the FTC has already logged over half a million consumer complaints related to COVID-19 and stimulus payments. Fraud and identity theft has made up 73 percent of these complaints, costing consumers more than $460 million. Consumers should be on the lookout for any communication from "government agencies" with instructions to click a link, pay a fee or provide personal identifying information (PII), such as a Social Security Number or banking information. Also, beware of social media scams, such as Facebook messages or Instagram posts that make offers of COVID-19 financial relief grants.

The FTC maintains a website warning consumers about the most up-to-date known pandemic scams, which is found here: https://www.ftc.gov/coronavirus/scams-consumer-advice. The website provides guidance for consumers to responsibly identify and respond to COVID-19 scams. FTC tips include: understanding that legitimate contact tracers need health information, but will not ask for money or personal financial information; disregarding unsolicited offers for vaccinations; ignoring advertisements for miracle treatments or cures; understanding that advertised test kits may not have not been approved by FDA; hanging up on robocalls; and being cognizant of the type of institution where someone is asking you to send your money.

Examples of COVID-19 Scams:

- **Contact Tracing** – In order to help track the spread of COVID-19, state health departments

have been employing contact tracers to reach those who have been exposed to the virus. Unfortunately, scammers have taken this opportunity to steal money and personally identifiable information from seniors and others. If you have concerns about whether someone who is contacting you is a real contact tracer from your state, check with your state health department to see if they can help.

- **Virus and Antibody Test Kits** – In the midst of the pandemic, many people are looking for ways to determine whether or not they may have contracted COVID-19. However, it is important to ensure that you only use tests from an official testing site (check with your state or local health department) or from your trusted medical professional. The FTC has advised that the public should be cautious of ads for test kits, as many of them have not been approved by the FDA and may not yield accurate results.
- **Vaccines** – As vaccine distribution continues, scammers are likely to take advantage of the system. The best way to find out information about COVID-19 vaccines, their availability in your state and other related information is to check the Centers for Disease Control and Prevention (CDC) website or consult your state health department. If you are contacted by someone offering you a vaccine, remember you do not need to pay money to be vaccinated, nor will anyone ask for your Social Security Number or banking information to schedule a vaccine appointment.
- **Miracle Cures** – Seniors should beware of products fraudulently marketed as the solution to COVID-19. Throughout the pandemic, some companies have peddled products that they allege will treat or cure the virus, without scientific proof substantiating their claims or FDA approval.

The Rise of Romance Scams Amid the COVID-19 Pandemic

The unexpected effects on society during the COVID-19 pandemic have unquestionably been innumerable. While the nation adapted to remote work, people also moved their social lives online. Isolation during the pandemic drove people of all ages to seek companionship, but unfortunately, scammers learned to adapt as well. Romance scams are a type of confidence fraud, where bad actors play towards their victims' emotional susceptibility to gain their trust.

During the pandemic, scammers learned to change their stories to include tall tales such as health problems, job losses and inability to travel in order to elicit sympathy from their victims, play on their compassion and access their money. This led to a rise in the number of calls to the Committee's fraud line reporting this type of scam.

It is understandable that romance scams specifically and confidence scams in general, are largely underreported due to victim embarrassment. Romance scams reported to the FBI have resulted in one of the highest amounts of financial losses when compared to other online fraud. Many scammers follow predictable practices when selecting and interacting with potential victims.

Reports collected by the FTC from consumers and local law enforcement show how sharply online romance fraud is increasing. In 2015, the agency received 8,500 such complaints. In 2019, the number topped 25,000.

Tips, Tricks & Telltale Signs – How To Spot A Romance Scammer

- Scammers can use details shared on social media and dating sites to better understand and target you.
- Research the person's photo and profile using online searches to see if the image, name or details have been used elsewhere.
- Protect photos of yourself and your loved ones. Use discretion and good judgment when sending images to someone you have not met. It is wise to avoid sending pictures completely until you have met the individual in person.
- Go slowly and ask lots of questions. Scammers tend to fall in love fast; beware of unlikely claims of "destiny" and "fate."
- Beware if the individual seems too perfect, or quickly asks you to communicate "offline."
- Beware if the individual attempts to isolate you from friends and family.
- Listen for foreign-based callers. Beware if the individual claims to be working and living far away, whether it is on the other side of the country or overseas.
- Beware if the individual is continuously available and overly responsive at any time of day or night.
- Beware if the individual promises to meet in person, but then always cancels because of some conflict or emergency.
- Beware if you are asked to send inappropriate photos or financial information that could later be used to extort you.
- Never send money to anyone you do not know personally.
- Never help anyone move money through your own account or someone else's. You could become an unwitting money mule for the perpetrator helping to carry out other theft and fraud schemes.

The Federal Bureau of Investigation (FBI) has recommended consumers be aware of common techniques used by romance scammers, which include:

- Claiming to be from the U.S. but currently living, working or traveling abroad.
- Claiming the romance was "destiny" or "fate," especially in early correspondence.
- Asking for money, goods, or similar types of financial assistance, especially if you have never met in person.
- Asking for assistance with personal transactions (opening a new bank account, depositing or transferring funds, shipping merchandise, etc.).

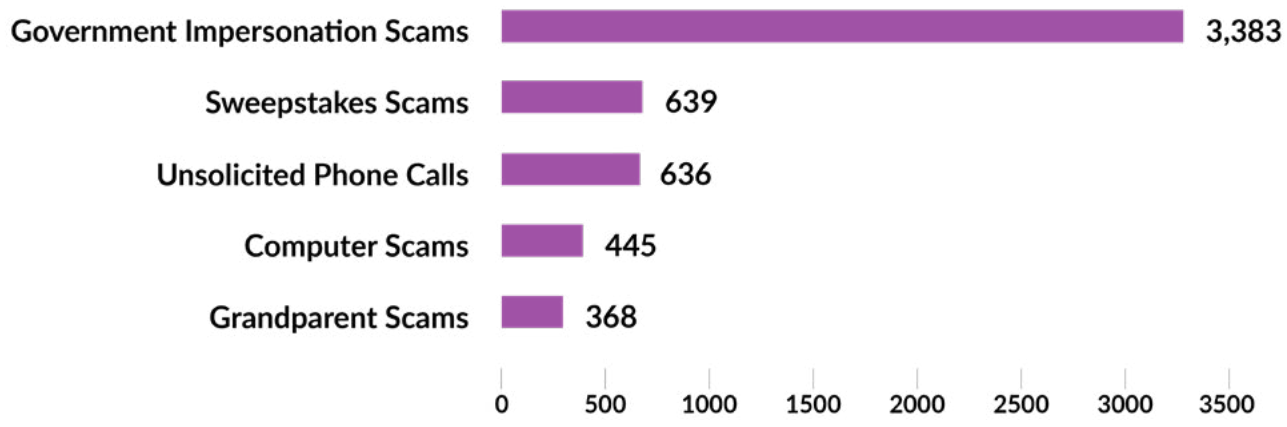
More tips available at the FBI Internet Crime Complaint Center's website at: https://www.ic3.gov/Home/ConsumerAlerts

Top 5 Scams Reported to the Aging Committee's Fraud Hotline, 2015-2020

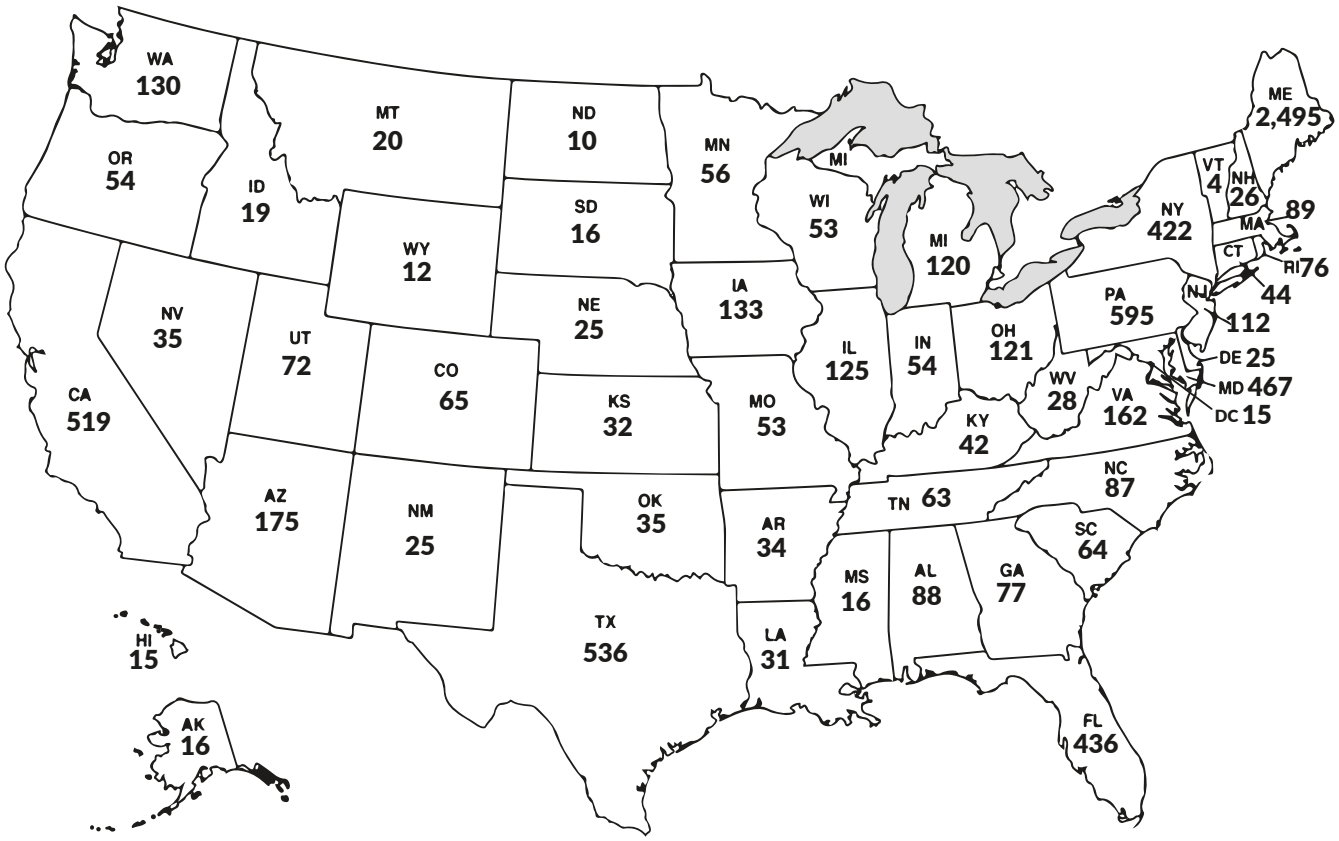
From January 1, 2015, through December 31, 2020, the Committee's Fraud Hotline received a total of 8,402 complaints from residents all across the country. Calls pertaining to the top 5 scams featured in this report account for more than 65 percent of the complaints.

Rank	Type of Scam	# of Complaints
1	Government Impersonation Scam	3,383
2	Sweepstakes Scams	639
3	Illegal Robocalls/Unsolicited Phone Calls	636
4	Computer Scams	445
5	Grandparent Scams	368

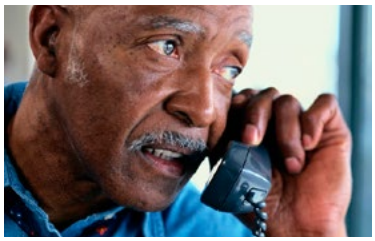
Top 5 Scams Reported to the Aging Committee, 2015-2020



Origin of Calls Received by the Aging Committee Fraud Hotline, 2015-2020



Top Five Scams Reported to the Aging Committee's Fraud Hotline, 2015-2020



1 Government Impersonation Scams

Fraud Case

A 58-year-old woman from North Ogden, Utah, received an alarming call from a man who claimed to be with the U.S. Drug Enforcement Agency (DEA). The scammer told the woman that she was under investigation on an international level and her Social Security Number was compromised. The fraudulent DEA agent informed her that she was unable to contact anyone in regards to this case, and that in order to keep her family safe, she needed to transfer her life savings and other money to a "safe place offshore." The self-proclaimed agent instructed her to go to the bank, withdraw her entire savings and wire the money to the agent. The woman, scared for herself and family, went to the bank and followed the man's instructions by transferring a total of $153,706. When she realized she had been scammed, she was devastated from losing her entire savings and contacted the FBI to report the crime.

Government impersonation scams frequently begin with a call from a scammer posing as an employee of a government agency, who may also "spoof" the call by using technology to make their caller ID appear as if they are calling from that agency. However, the scammer makes requests and demands that a government employee would never make. For example, the scammer may threaten the senior, demand immediate payment, or require a specific means of payment, such as a wire transfer, prepaid debit card, retail gift card or cash. These scams can take various forms.

These often convincing scams can lead to identity theft, which is a wide-ranging fraud category that can include calls about theft of a wallet or mail, online impersonation or other illegal efforts to obtain a person's sensitive information. Identity thieves not only disrupt the lives of individuals by draining bank accounts, making unauthorized credit card charges and damaging credit reports, but can also defraud the government and taxpayers by using stolen personal information to submit fraudulent billings to Medicare or Medicaid, or apply for and receive Social Security benefits to which they are not entitled. Scammers also use stolen personal information, including Social Security Numbers, to commit tax fraud, benefits fraud, unemployment insurance fraud or to fraudulently apply for jobs and earn wages.

Internal Revenue Service Scams

Another common type of government impersonation scam occurs when criminals make contact claiming to be an employee from the Internal Revenue Service (IRS). While there are multiple variations of this scam, criminals generally accuse victims of owing back taxes and penalties. They also may threaten retaliation, such as arrest or deportation, if immediate payment is not made by certified check, wire transfer or gift card.

Many times, after a victim makes an initial payment, they are told that upon further review of their records, another discrepancy has been identified and they must pay an additional sum of money to resolve that difference or else face adverse action. Scammers may take victims through this process multiple times. In contrast, the true IRS normally contacts consumers through a letter mailed by the U.S. Postal Service. Calls may be made by IRS representatives depending on the situation, but each representative can provide two forms of official credentials.

Social Security Scams

Many seniors have been contacted by scammers pretending to be the Social Security Administration (SSA). There are several variations to this scam, but the general theme involves scammers calling victims to fraudulently take money from them or obtain their personally identifiable information, such as a Social Security Number. The scammers will attempt to scare consumers by claiming that their Social Security Number has been suspended due to suspicious activity or has been used in a crime. The caller may even threaten a lawsuit if the information they demand is not provided. The scammers will say the situation can only be resolved by providing sensitive personal information over the phone or by paying a sum of money using certain forms of payment such as gift cards. These tactics aim to cause the consumer to panic by creating a false sense of urgency in hopes that the consumer will give away their personal information and money. (See scam call script above for an example.)

Social Security Callback Scam - CALL SCRIPT

"Hello this is a call from the Social Security Administration. During these difficult times of the coronavirus, we regret to inform you that we have got an order to suspend your Social Security payments immediately within 24 hours due to suspicious and fraudulent activity. We are contacting you as this case is critical and needs your urgent attention. To get more information about this case please call immediately on our department number 888-991-XXXX. I repeat 888-991-XXXX."

While SSA employees do occasionally reach out to beneficiaries by telephone for business purposes, such calls are typically placed to individuals who have ongoing business with the agency. As a result, a legitimate call from the agency would be on a topic previously known to the person receiving the call, whereas a scam call would be out of the blue.[1] While this scam has also been perpetuated via email, the SSA notes that the agency will *not* reach out to ask for personal identifiable information over email.[2]

What to do if you're suspicious of a government impersonation scam

Scammers will try to get personal identifiable information in many ways and through different types of scams. In some cases, thieves can illegally access an existing customer's account simply by entering that individual's username or email address and correctly guessing their password. This is often referred to as an "account takeover." Additionally, medical identity theft occurs when someone steals personal information to obtain medical care, buy prescription drugs or submit fake billings to Medicare.

If you are unsure whether you are speaking with a real government representative, you can hang up or request that they call you back later after verifying the call is legitimate through official means. To contact the Social Security Administration, call the SSA Inspector General's Office at 1-800-772-1213.[3]

For the Internal Revenue Service: if you owe (or think you owe) taxes call 1-800-829-1040. If you do not owe taxes, call the Treasury Inspector General for Tax Administration at 1-800-366-4484 to report the impersonation.[4]

Tips to Remember:

- Medicare and Social Security will not call you to ask for your bank information or Social Security Number.
- There will never be a fee charged to obtain a Social Security or Medicare card.
- Never give out personal information over the phone.
- Sensitive personal and financial documents should be kept secure at all times.
- Review all medical bills to spot any services that you didn't receive.

The Federal Trade Commission (FTC) has given the following tips to help consumers avoid government impostor scams:

- Be aware - scammers often pressure people into wiring money, putting money on a prepaid debit card, or sending a check or money order using an overnight delivery or courier service.
- Never give out or confirm financial or other sensitive information unless you know who you're dealing with.
- Don't trust a name or number. Scammers use official-sounding names to make you trust them. And to make their call seem legitimate, scammers also use technology to disguise their real phone number.

For more helpful tips, please visit the FTC's website at: https://www.consumer.ftc.gov/articles/0048-government-imposter-scams

Do You Think You Have Been Scammed?

What to Do *Right Away:*

1. **Call the companies** where you know the fraud occurred.
2. **Place a fraud alert** with a credit reporting agency and get your credit report from one of the three national credit bureaus.
3. **Report identity theft** to the Federal Trade Commission.
4. **File a report** with your local police department.

What to Do *Next:*

1. **Close new accounts** opened in your name.
2. **Remove bogus charges** from your accounts.
3. **Correct** your credit report.
4. **Consider** adding an extended fraud freeze.

2 Sweepstakes Scams

Fraud Case

An 89-year-old woman from Bluffton, South Carolina, received a letter from "Mega Millions" that claimed she was the lucky winner of $2.5 million and a brand-new Mercedes-Benz convertible. In order to claim her prize, the letter instructed the woman to wire a one-time payment of $16,000 to the telephone number listed. When the woman called the number, she shared her debit card information and the proclaimed lottery agent withdrew $16,000. Sadly, the woman never received more information or the millions of dollars and new convertible she was told she had won.

Sweepstakes scams intend to steal from seniors who believe they have won a lottery and only need to take a few actions to obtain their winnings. In this scam, fraudsters generally contact victims by phone or through the mail to tell them that they have won or have entered to win a prize. Scammers then require the victims to pay a fee or the taxes to either collect their supposed winnings or improve their odds of winning the prize.[5]

Typically, scammers tell victims that they have won the lottery or a brand new car. In order for their winnings to be claimed, victims are told they must first wire a few hundred to a few thousand dollars to cover processing fees and taxes. The criminals will often instruct victims not to share the good news with anyone so that it will be a "surprise" to their families. Scammers tell victims to send money in various ways, including gift cards, electronic wire transfers, money orders and cash.

Scammers have been known to impersonate well-known sweepstakes or contest organizations (such as Publishers Clearing House) to make this scam seem more realistic. Scammers will even claim to be an executive in the company and may spend hours on the phone to develop a relationship with the victim. In this scam, no winnings are ever delivered and the "winners" get nothing but more scam calls. Some victims have reported up to 100 calls per day from scammers demanding additional money.

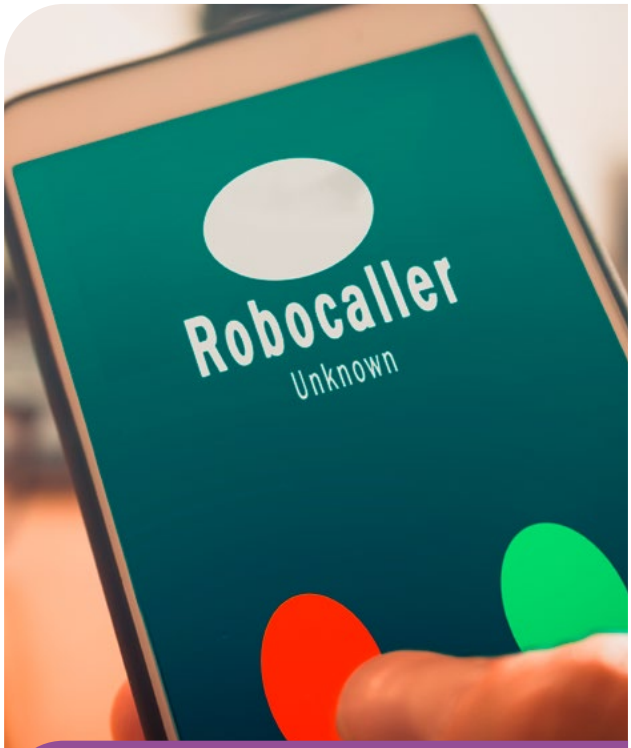
Many times, con artists adopt a variety of identities to keep the money coming in ever-increasing amounts and convince the victim that their winnings will come soon if they continue to send money. Victims who resist their requests have reported that they began receiving calls from scammers posing as American government officials, including local law enforcement, the Federal Bureau of Investigation, the Social Security Administration and the Department of Homeland Security asking for personal data and bank account numbers so they can "solve" the crime.

The Federal Trade Commission (FTC) has given the following tips to help consumers avoid government imposter scams:

- Be aware - scammers often pressure people into wiring money, putting money on a prepaid debit card or sending a check or money order using an overnight delivery or courier service.
- Never give out or confirm financial or other sensitive information unless you know who you're dealing with.
- Don't trust a name or number. Scammers use official-sounding names to make you trust them. And to make their call seem legitimate, scammers also use technology to disguise their real phone number.

For more helpful tips, please visit the FTC's website at: https://www.consumer.ftc.gov/articles/0048-government-imposter-scams

3 Illegal Robocalls and Unsolicited Phone Calls



Fraud Case

An 82-year-old woman from Atlanta, Georgia, was the victim of ongoing robocalls. She constantly received calls from individuals who claimed she had won large cash prizes and required her to send a one-time payment in order to receive her prize. The woman took these calls and believed all the individuals who had contacted her. Devastatingly, she lost her life savings and took out a reverse mortgage on her home in order to pay the scammers.

Despite the federal government's best efforts, illegal robocalls continue to plague consumers across the nation, including seniors.[6] Robocalling is the process of using technology to mechanically, as opposed to manually, dial phone numbers in sequence. While there are legal uses for robocalls, robocalls can still be used for nefarious and illegal purposes. These perpetrators can use robocall technology to make a large number of these calls per day at a low cost. But these calls are not just illegal or annoying; scammers use them to find potential victims.

Robodialers can be used to distribute prerecorded messages or to connect the person who answers the call with a live caller. Robocalls often originate overseas, but consumers often do not know because scammers usually spoof the number from which they are calling to either mask their true identity or to take on a new one, in order to make victims believe they are calling from the government or another legitimate entity. Additionally, scammers might spoof numbers to make it appear as if they are calling from a local area code.

If you are a victim of illegal robocalls, report it to the FCC at 888-225-5322 and to the FTC at 877-382-4357.

Impending Lawsuit Scams

Similar to the IRS impersonation or Social Security impersonation scams, impending lawsuit scams typically involve victims receiving calls from individuals claiming to be from local, state, or federal government or a law enforcement agency. Consumers are told that there is a warrant out for their arrest or that they will be sued unless they agree to pay a fine. A common version of this scam is the scammer claiming an arrest warrant was issued for failing to report for jury duty. To give the calls more credibility, scammers will often spoof the phone number so caller-ID appears to show that the call is coming from a legitimate agency, such as the local police department.

Usually, the caller imposes a deadline, such as the end of the business day, to create a sense of urgency and fear on behalf of the victim. Scammers will claim multiple attempts have been made to notify the victim but were missed or never received for some reason and then demand payment to resolve the issue. Some versions of this scam attempt to fluster the victims or make them react without thinking, while other variations have scammers calmly asking for personal information that is then sold to identity thieves.

The Federal Communications Commission (FCC) has published the following tips to help consumers avoid spoofing:

- Don't 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 spoofed. Be aware: Caller ID showing a "local" number does not necessarily mean it is a local caller.
- Do not respond to any questions, especially those that can be answered with "Yes."
- 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.
- 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 get an inquiry from someone who says they represent a company or government agency, hang up and call the phone number on your account statement, in the phone book or on the company's or government agency's website to verify the authenticity of the request. You will usually get a written statement in the mail before you get a phone call from a legitimate source, particularly if the caller is asking for a payment.

More tips available at the FCC's website at: https://www.fcc.gov/consumers/guides/spoofing-and-caller-id

4 Computer Tech Scams

Fraud Case

A 76-year-old woman who was relatively familiar with technology received a yellow flashing alert on her laptop one day stating that hackers had taken control of her device and to call the number that was provided on her screen. The woman proceeded to call the number immediately, and a man answered the phone claiming he was tech support.

The tech agent requested that she send $2,000 in order to relieve her computer of hackers and she did just that. After the fact, she contacted her daughter, who told her mother that she had been scammed. The 76-year-old woman's bank informed her that they were not able to recover the lost amount and there was nothing they could do for her.

Computer-based scams involve con artists trying to gain the victims' trust by pretending to be associated with a well-known technology company, such as Microsoft, Apple or Dell. They may use tactics such as falsely claiming that the victim's computer has been infected with a virus. Scammers then convince victims to provide remote access to their computers, personal information or credit card and bank account numbers so that victims can be "billed" for fraudulent services to fix the virus.

In a computer tech scam, an individual, while searching the internet, may suddenly get a pop-up window on their computer screen describing a security threat and instructing them to contact a tech support agent. Sometimes, scammers have used the pop-up window to hack into a victim's computers, lock them out and force the victim to pay a ransom to regain control of their computer. Below are several of the most common variations of this scam:

- **Scammers Contact Victims.** In the most prevalent variation of this scam, con artists randomly call potential victims and offer to clean their computers and/or sell them a long-term or technical support "service." The scammers also spread viruses that cause the victims' computers to display error messages that pop up onto the screen, instructing them to call a number to fix the problem. Scammers generally charge victims hundreds of dollars and may install free programs or trial versions of antivirus programs to give the illusion that they are repairing the computers. If victims express concern about the price, the con artists

will often entice victims to pay by offering a "senior citizen discount."

- **Victims Unknowingly Contact Scammers.** Some consumers unknowingly call a fraudulent tech support number after viewing the phone number online. Consumers who search for tech support online may see the number for the scammer at the top of their search results, called "sponsored results." Some key search terms include: "virus removal," "how to get rid of a computer virus," "McAfee Customer Support," and "Norton Support." These search terms are cleverly chosen to confuse the consumer into thinking the scammers are associated with well-known companies.

Legitimate companies do not display pop-up warnings asking you to call a toll-free number about viruses or security problems.

- **Fraudulent Refund.** Scammers contact victims stating that they are owed a refund for prior services. The scammers generally convince victims to provide them with access to their computers to process an online wire transfer. Instead of refunding the money, the fraudsters use the victims' account information to steal their savings or commit identity theft.
- **Ransomware.** Scammers use malware or spyware to infect victims' computers with a virus or encrypt the computers so they cannot be used until a fee is paid. If victims refuse to pay, scammers will render the computer useless, sometimes prompting a blue screen that can only be removed with a password known by the scammers. The Fraud Hotline has received reports that scammers have admitted to victims that it is a scam and refuse to unlock the victims' computers unless a "ransom" payment is made.[7]

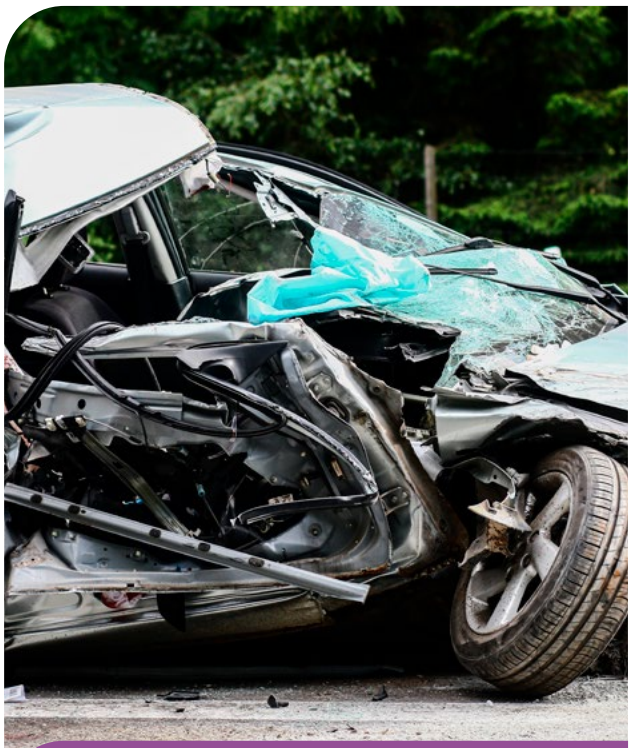
Tips from the Federal Trade Commission (FTC) to help consumers avoid becoming a victim of a computer-based scam:

If you get a pop-up or spam email about a virus on your computer:

- Don't click on any links or call a phone number.
- Don't send any money or make a wire transfer.
- Don't pay with a gift card.
- Don't give anyone your bank account, credit card number or other payment information.
- Don't give anyone control of your computer.
- If you need help fixing a problem, go to someone you know and trust to help you.

More tips available at the FTC's website at: https://www.consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams

5 Grandparent Scams



Fraud Case

A woman from Colorado Springs, Colorado received a call from a young man who claimed to be her grandson. His voice was muffled and trembling. The imposter shared that he was involved in a car accident and had been rushed to the hospital. He told the woman he would be taken to jail after being discharged from the hospital if he did not provide the officers with $2,500 for bail onsite.

The woman was shocked and decided to wire the requested amount to the young man who she believed to be her grandson. She later called her grandson on his personal cell number and discovered that her grandson never called asking for assistance and had never been in an accident.

A common scam used to target older Americans is the "grandparent scam." In this scam, imposters either pretend to be the victim's grandchild or a law enforcement officer detaining the victim's grandchild. The scammers 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 their victims' emotions and trick concerned grandparents into wiring money to them. For example, in a January 2019 Aging Committee hearing, a Pennsylvania witness shared the story of her parents losing over $80,000 to a scammer who convinced them that their grandson had been arrested and jailed.[8] The Fraud Hotline has received frequent reports of con artists telling victims their family member was pulled over by the police and arrested after drugs were found in the car. The scammer who is pretending to be the victim's grandchild will often tell the victim to refrain from alerting the grandchild's parents. Additionally, the Fraud Hotline has received reports of imposter grandchildren claiming to have broken their noses in car accidents to explain why their voices sound different.

Criminals pressure their victims for urgent help, pressuring their targets to send money in the fastest way possible. This typically requires the victim to go

If you are contacted by a family member who claims to be in trouble with the law or in need of other financial assistance, call their number or check with other family members before sending money to help.

to a local retailer and send an electric wire transfer of several thousand dollars, but other methods like gift cards and cash are also used. After payment has been made, the fraudster will likely call the victim back, claiming that there was another legal fee of which they were not initially aware.

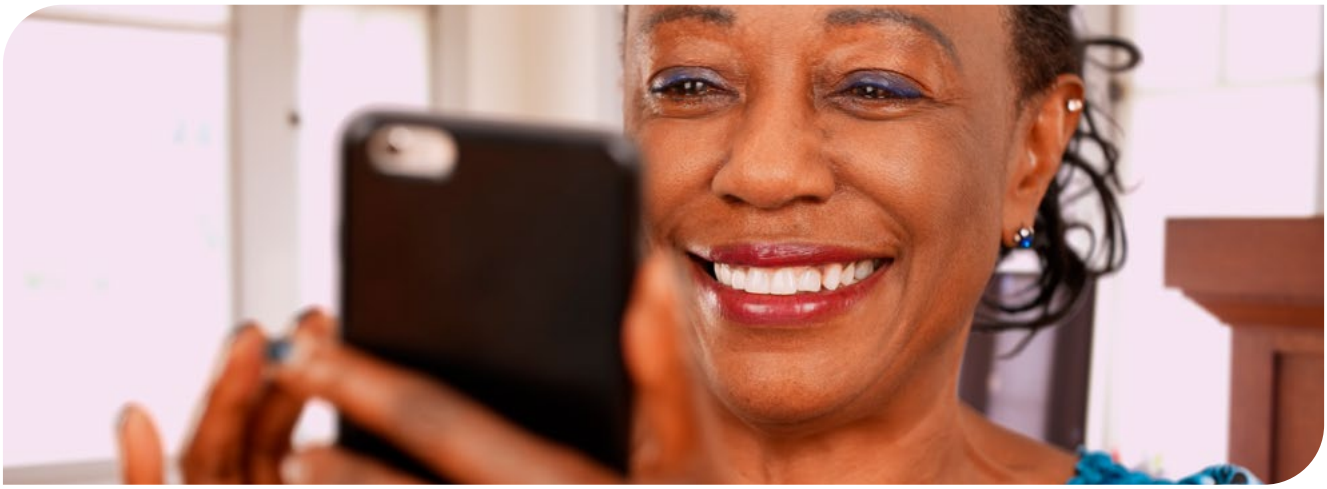
In another version of the scam, instead of the "grandchild" making the phone call, the con artist pretends to be an arresting police officer, a lawyer or a doctor. It is also common for the scammer impersonating the victim's grandchild to talk briefly with the scam victim and then hand the phone over to an accomplice impersonating an authority figure. This gives scammer stories more credibility and reduces the chance the victim will recognize that the voice on the phone does not belong to their grandchild.

Tips from the Federal Trade Commission (FTC) to help consumers avoid becoming a victim of the "grandparent" or "family emergency" scam:

- Resist the urge to act immediately, no matter how dramatic the story is.
- Verify the person's identity by asking questions that a stranger couldn't possibly answer.
- Call a phone number for your family member or friend that you know to be genuine.
- Check the story out with someone else in your family or circle of friends, even if you've been told to keep it a secret.

More tips available at the FTC's website at: https://www.consumer.ftc.gov/articles/0204-family-emergency-scams

How to Protect Yourself



While the scams highlighted in this book continue to be used by fraudsters, they are not the only types of scams. Scammers regularly create and utilize new schemes to defraud consumers, including seniors. There are steps seniors can take to help avoid falling victim to various types of scams, which are outlined in the tip cards, pull-out poster and otherwise throughout this book.

Overall, it is important that seniors stay alert against any efforts to steal their money. For example, since most scams originate with a phone call, seniors must remain aware when taking phone calls and hang up immediately if the caller sounds suspicious, makes threats or makes an offer that sounds too good to be true or requires something in return. Consumers should also carefully read any contract, or consult with others, before agreeing to sign. Generally, in order to avoid losing money to any type of scam, it is important to keep the following tips in mind:

Tips for Avoiding Phone Scams

To convince you to give them money and personal information, con artists will often:

- Force you to make decisions fast.
- Threaten you.
- Use fake caller IDs to disguise their real numbers.
- Pretend to be a government employee (e.g. IRS or Social Security Administration).
- Pressure you not to consult with friends and family.
- Urge you to hand over personal information like your Social Security Number or account numbers.
- Always remember: if an offer sounds too good to be true, it most likely is!

If you receive a suspicious call, hang up and call the U.S. Senate Special Committee on Aging's Fraud Hotline at 1-855-303-9470.

Fraud Resources

The staff on the Committee's Fraud Hotline (1-855-303-9470) are available to provide you with direction if you experience suspicious activity. The Fraud Hotline is staffed Monday through Friday, 9 AM to 5 PM ET. The following are additional channels of support.

For Identity Theft

Call one of the three national credit bureaus to place a fraud alert.

Equifax	1-800-685-1111 (Fraud Hotline: 1-888-766-0008)
Experian	1-888-397-3742 (Fraud Hotline: 1-888-397-3742)
TransUnion	1-800-916-8800 (Fraud Hotline: 1-800-680-7289)

From Relevant Consumer Agencies and Organizations

Agency	Website	Phone Number
Better Business Bureau (BBB)	www.bbb.org	Use zip code to find local BBB
National Do-Not-Call Registry	https://www.donotcall.gov/	1-888-382-1222
Eldercare Locator (U.S. Administration on Aging)	https://eldercare.acl.gov/	1-800-677-1116
AARP Fraud Watch Network	www.aarp.org/fraudwatchnetwork	1-800-646-2283
Federal Trade Commission	http://www.consumer.ftc.gov/	1-877-382-4357
U.S. Department of Justice (DOJ) Elder Justice Initiative	www.justice.gov/elderjustice/	1-833–372–8311
Medicare Fraud Hotline (CMS)	https://www.medicare.gov/forms-help-resources/help-fight-medicare-fraud/how-report-medicare-fraud	1-800-633-4227 TTY: 877-486-2048
Social Security Administration Office of Inspector General	https://oig.ssa.gov/	1-800-269-0271

State Attorneys General

If you think you have been defrauded by a business or had assets stolen by someone you trusted, call your state or territory Attorney General's office.

State/Territory	Phone Number
Alabama	(334) 242-7300
Alaska	(907) 269-5100
America Samoa	(684) 633-4163
Arizona	(602) 542-5025
Arkansas	(800) 482-8982
California	(916) 445-9555
Colorado	(720) 508-6022
Connecticut	(860) 808-5400
Delaware	(302) 577-8600
District of Columbia	(202) 442-9828
Florida	(850) 414-3300
Georgia	(404) 656-3300
Guam	(671) 475-2720
Hawaii	(808) 586-1500
Idaho	(208) 334-2400
Illinois	(312) 814-3000
Indiana	(317) 232-6330
Iowa	(515) 281-5044
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
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	(802) 828-3173
Virginia	(804) 786-2071
Washington	(360) 753-6200
West Virginia	(304) 558-2021
Wisconsin	(608) 266-1221
Wyoming	(307) 777-7841

Appendix A: Aging Fraud Hotline Calls by Scam Type, 2015-2020

Scam	Number
Bad Business Practices	25
Bad Landlord	2
Bank Fraud	36
Can you hear me? Scams	123
Charity Scam	71
Check Scam	79
Computer Scam	445
Consumer Related	124
Counterfeit Scam	3
COVID Scam	5
Debt Collection Scam	87
Dietary Supplements Scam	1
Disability Enrollment Scam	1
DME Scam	5
Elder Abuse	268
Elder Financial Abuse	59
Fraud Book Request	4
Free Trial Scam	1
Government Grant	152
Grand Jury Impersonation Scam	5
Grandparent Scam	368
Health Related Scam	84
Home Improvement Scam	36
Identity Theft	231
Immigration Scam	1
Impending Lawsuits	108
Inheritance Scam	21
Insurance Fraud	1
Int'l Drug Trafficking Scam	1
Investment Fraud	43
IRS Fraudulent Tax Returns	22
IRS Impersonation Scam	3,015
Jamaican Lottery Scam	2
Junk Mail	7
Kidnapping Scam	5
Left no VM	10
Legal Referral	28
Life Insurance Scam	1
Long-term Care	2
Mail Scam	44
Medical Equipment	3
Military Impersonation Scam	1
Miscellaneous	663
Mortgage Fraud	35
Nigerian Gold Scam	2
Nigerian Prince Inheritance	3
Online VA Impersonation Scam	1
Payday Lending	5
Pension/Retirement Fraud	11
Phishing Scam	21
Robbery/Theft	7
Romance Scam	314
SMishing Scam	2
Social Security	368
Spam email	37
SSDI Issues	1
Sweepstakes Scam	639
Timeshare Scam	26
Unclaimed Property Scam	7
Unsolicited Phone Calls	636
Utility Scam	62
Wire Fraud	32
TOTAL CALLS:	**8,402**

Appendix B: Aging Fraud Hotline Calls by State/Territory, 2015-2020

State	Number
Alabama	88
Alaska	16
Arizona	175
Arkansas	34
California	519
Colorado	65
Connecticut	44
Delaware	25
District of Columbia	15
Florida	436
Georgia	77
Hawaii	15
Idaho	19
Illinois	125
Indiana	54
Iowa	133
Kansas	32
Kentucky	42
Louisiana	31
Maine	2,495
Maryland	467
Massachusetts	89
Michigan	120
Minnesota	56
Mississippi	16
Missouri	53
Montana	20
Nebraska	25
Nevada	35
New Hampshire	26
New Jersey	112
New Mexico	25
New York	422
North Carolina	87
North Dakota	10
Ohio	121
Oklahoma	37
Oregon	54
Pennsylvania	595
Rhode Island	76
South Carolina	64
South Dakota	16
Tennessee	63
Texas	536
Utah	72
Vermont	4
Virginia	162
Washington	130
West Virginia	28
Wisconsin	53
Wyoming	12
Unknown	376
TOTAL CALLS:	**8,402**

Appendix C: Aging Fraud Hotline Statistics, 2020

State	Number
Alabama	13
Alaska	1
Arizona	8
Arkansas	0
California	21
Colorado	3
Connecticut	3
Delaware	2
District of Columbia	2
Florida	25
Georgia	6
Hawaii	0
Idaho	0
Illinois	8
Indiana	5
Iowa	2
Kansas	0
Kentucky	6
Louisiana	6
Maine	129
Maryland	14
Massachusetts	10
Michigan	9
Minnesota	5
Mississippi	0
Missouri	3
Montana	3
Nebraska	4
Nevada	1
New Hampshire	3
New Jersey	6
New Mexico	0
New York	29
North Carolina	5
North Dakota	0
Ohio	10
Oklahoma	3
Oregon	6
Pennsylvania	50
Rhode Island	2
South Carolina	2
South Dakota	0
Tennessee	6
Texas	24
Utah	2
Vermont	1
Virginia	8
Washington	2
West Virginia	2
Wisconsin	2
Wyoming	0
Unknown	154
TOTAL CALLS:	**606**

Scam Type	Number
Social Security	226
Romance Scam	50
Computer Scam	38
Consumer Related	38
Grandparent Scam	37
Sweepstakes Scam	37
Miscellaneous	18
Utility Scam	18
Debt Collection Scam	13
Government Grant	13
Unsolicited Phone Calls	13
Identity Theft	11
Left no VM	10
Health Related Scam	9
Elder Abuse	8
Investment Fraud	8
Phishing Scam	8
Check Scam	6
Inheritance Scam	6
Charity Scam	5
COVID Scam	5
Fraud Book Request	4
Robbery/Theft	4
Timeshare Scam	4
Bank Fraud	3
DME Scam	3
IRS Scam	3
Mortgage Fraud	3
Jamaican Lottery Scam	2
Mail Scam	2
Pension/Retirement Savings Fraud	1

2020 TOTAL:	606

Tips from the United States Senate Special Committee on Aging for

Avoiding Scams

- Con artists force you to make decisions fast and may threaten you.
- Con artists disguise their real numbers, using fake caller IDs.
- Con artists sometimes pretend to be the government (e.g. IRS).
- Con artists try to get you to provide them personal information like your Social Security number or account numbers.
- Before giving out your credit card number or money, please ask a friend or family member about it.
- Beware of offers of free travel!

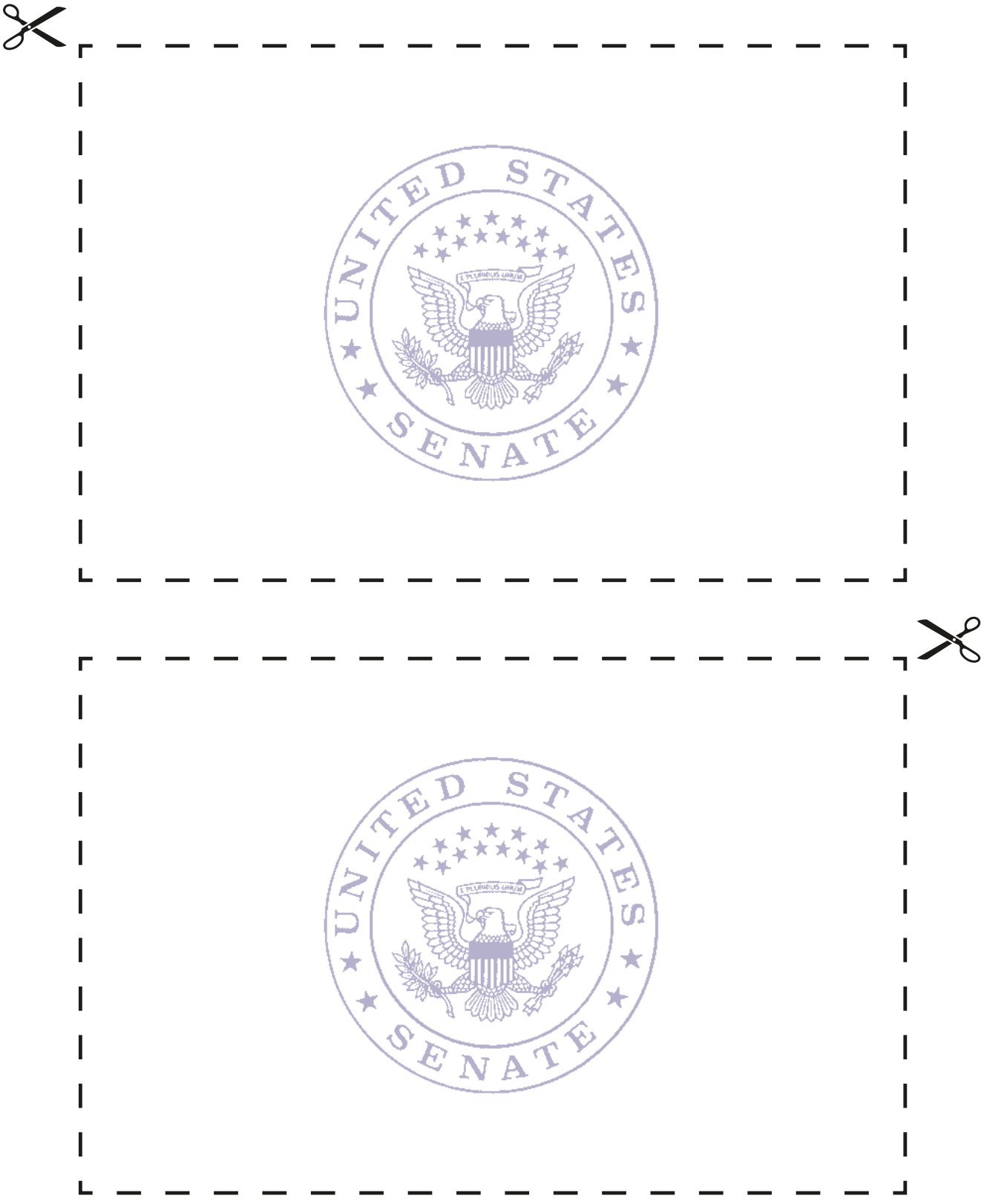
If you receive a suspicious call, hang up and please call the U.S. Senate Special Committee on Aging's Fraud Hotline at 1-855-303-9470

Tips from the United States Senate Special Committee on Aging for

Avoiding Scams

- Con artists force you to make decisions fast and may threaten you.
- Con artists disguise their real numbers, using fake caller IDs.
- Con artists sometimes pretend to be the government (e.g. IRS).
- Con artists try to get you to provide them personal information like your Social Security number or account numbers.
- Before giving out your credit card number or money, please ask a friend or family member about it.
- Beware of offers of free travel!

If you receive a suspicious call, hang up and please call the U.S. Senate Special Committee on Aging's Fraud Hotline at 1-855-303-9470



References

1 U.S. Social Security Administration, "Social Security Administration and its Inspector General Announce New Online Reporting Form for Imposter Scam Calls", November 19, 2019 https://www.ssa.gov/news/press/releases/2019/#11-2019-2

2 U.S. Social Security Administration, Information About Scams https://www.ssa.gov/phila/scams.htm

3 U.S. Social Security Administration, Information About Scams https://www.ssa.gov/phila/scams.htm

4 Treasury Inspector General for Tax Administration, "TIGTA Unveils New Flyer Warning Taxpayers About Impersonation Scam", March 5, 2020 https://www.treasury.gov/tigta/press/press_tigta-2020-01.htm

5 Federal Trade Commission, Fake Prize, Sweepstakes, and Lottery Scams https://www.consumer.ftc.gov/articles/fake-prize-sweepstakes-and-lottery-scams

6 "To ratify the authority of the Federal Trade Commission to establish a do-not-call registry." Public Law 108-82. 108th Congress, 1st sess.; https://www.fcc.gov/document/fcc-issues-report-illegal-robocalls

7 Federal Trade Commission, How To Spot, Avoid, and Report Tech Support Scams, https://www.consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams

8 U.S. Congress, Senate Special Committee on Aging, Fighting Elder Fraud: Progress Made, Work to be Done, hearings, 116th Cong., 1st sess., January 16, 2019 https://www.aging.senate.gov/imo/media/doc/SCA_Flavin_complete_01_16_19.pdf

Fraud Cases

Fraud case page 6: Michael Finney, Beware of COVID-19 vaccine phone scams, SF woman shares experience: Here's what you need to know, March 6, 2021, available at https://abc7news.com/7-on-your-side-7oys-michael-finney-consumer/10391988/, accessed June 22, 2021

Fraud case page 8: Sofastall, M. (2018, Sep 27). Victim of Romance Scam Cheated Out of $75,000 after Meeting the "Perfect guy" Online. Retrieved Jun 8, 2021 from https://www.foxcarolina.com/news/us_and_world/victim-of-romance-scam-cheated-out-of-75-000-after-meeting-the-perfect-guy-online/article_61f26586-f7d7-5b97-89a7-7f104c71da60.html

Fraud case page 14: McKellar K. (2019, Dec 26). 'He terrorized her': Aggressive Scammer Tricked Utah Woman to Turn over Life Savings. Retrieved Jun 8, 2021 from https://www.deseret.com/utah/2019/12/26/21038272/utah-lawmaker-scammed-scam-wife-fraud-dea-life-savings-kyle-andersen-machel

Fraud case page 17: Shore, J. (2020, Dec 03). Bluffton Mother, Son Charged in Alleged $700K Sweepstakes Fraud Targeting the Elderly. Retrieved Jun 8, 2021 from https://www.islandpacket.com/news/local/crime/article247559450.html

Fraud case page 19: 11Alive Staff, Woman blames rob callers in grandmother's death, 11Alive, 05/07/2021, Available at What happens if you answer a robocall? | https://www.11alive.com/, accessed 08/18/2021.

Fraud case page 21: Jennifer Jolly, This 'tech support' scam is stealing million from seniors, including my mom, USA Today, 04/09/2021, Available at How 'tech support' scam is stealing from seniors, including my mom (https://www.usatoday.com/), accessed 08/16/2021.

Fraud case page 23: Pelton, K. (2020, Feb 17). Voice of the Consumer: Woman Left Shaken by Grandparent Scam Call. Retrieved Jun 8, 2021 from https://www.kktv.com/content/news/Voice-of-the-consumer-Woman-left-shaken-by-grandparent-scam-call-567946271.html

Notes

Poster Here

Poster Here

Notes

If you receive a suspicious call, hang up and please call
the U.S. Senate Special Committee on Aging's Fraud Hotline at

1-855-303-9470