# United States Senate
# Special Committee on Aging

# Fighting Fraud:

## Senate Aging Committee Identifies

## **Top 10 Scams** Targeting Our Nation's Seniors

**Senator Susan M. Collins (R-ME), Chairman**
**Senator Robert P. Casey, Jr. (D-PA), Ranking Member**

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**

# Table of Contents

# Senate Special Committee on Aging

***SUSAN M. COLLINS, Maine***

*TIM SCOTT, South Carolina*

*RICHARD BURR, North Carolina*

*MARTHA MCSALLY, Arizona*

*MARCO RUBIO, Florida*

*JOSH HAWLEY, Missouri*

*MIKE BRAUN, Indiana*

*RICK SCOTT, Florida*

***ROBERT P. CASEY, JR., Pennsylvania***

*KIRSTEN GILLIBRAND, New York*

*RICHARD BLUMENTHAL, Connecticut*

*ELIZABETH WARREN, Massachusetts*

*DOUG JONES, Alabama*

*KYRSTEN SINEMA, Arizona*

*JACKY ROSEN, Nevada*

# Dear Friends,

It is estimated that older Americans lose a staggering $2.9 billion a year to an ever-growing array of financial exploitation schemes and scams. They are being targeted by criminals who want to rob them of their hard-earned retirement savings. They are being exploited by strangers over the telephone, through the mail, and online. Worse yet, far too many seniors may also be targeted by family members or by other people who they trust.

The U.S. Senate Special Committee on Aging is committed to protecting older Americas against fraud and to bringing greater awareness of this pervasive problem. The Committee maintains a toll-free Fraud Hotline: **1-855-303-9470**. By serving as a resource for seniors and others affected by scams, the Hotline has helped increase reporting and awareness of consumer fraud. Additionally, Committee staff and investigators who operate the Fraud Hotline can provide callers with important information to help reduce the likelihood that they will become a victim.

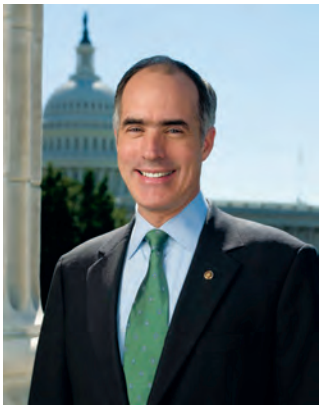
Over the past year, more than 1,500 individuals all across the country contacted the Fraud Hotline. Since the Fraud Hotline's inception in 2013, more than 8,200 individuals from all 50 states have contacted the Committee's Fraud Hotline to report a possible scam. The Committee would like to thank the many consumer advocacy organizations, community centers, and local law enforcement that have provided invaluable assistance by encouraging consumers to call the Fraud Hotline to document scams. We look forward to building upon our successful efforts to investigate and stop scams aimed our nation's seniors, and to ensure that federal agencies are aggressively pursuing the criminals who commit these frauds.

Sincerely,

Susan M. Collins

Robert P. Casey, Jr.

Susan M. Collins
*Chairman*



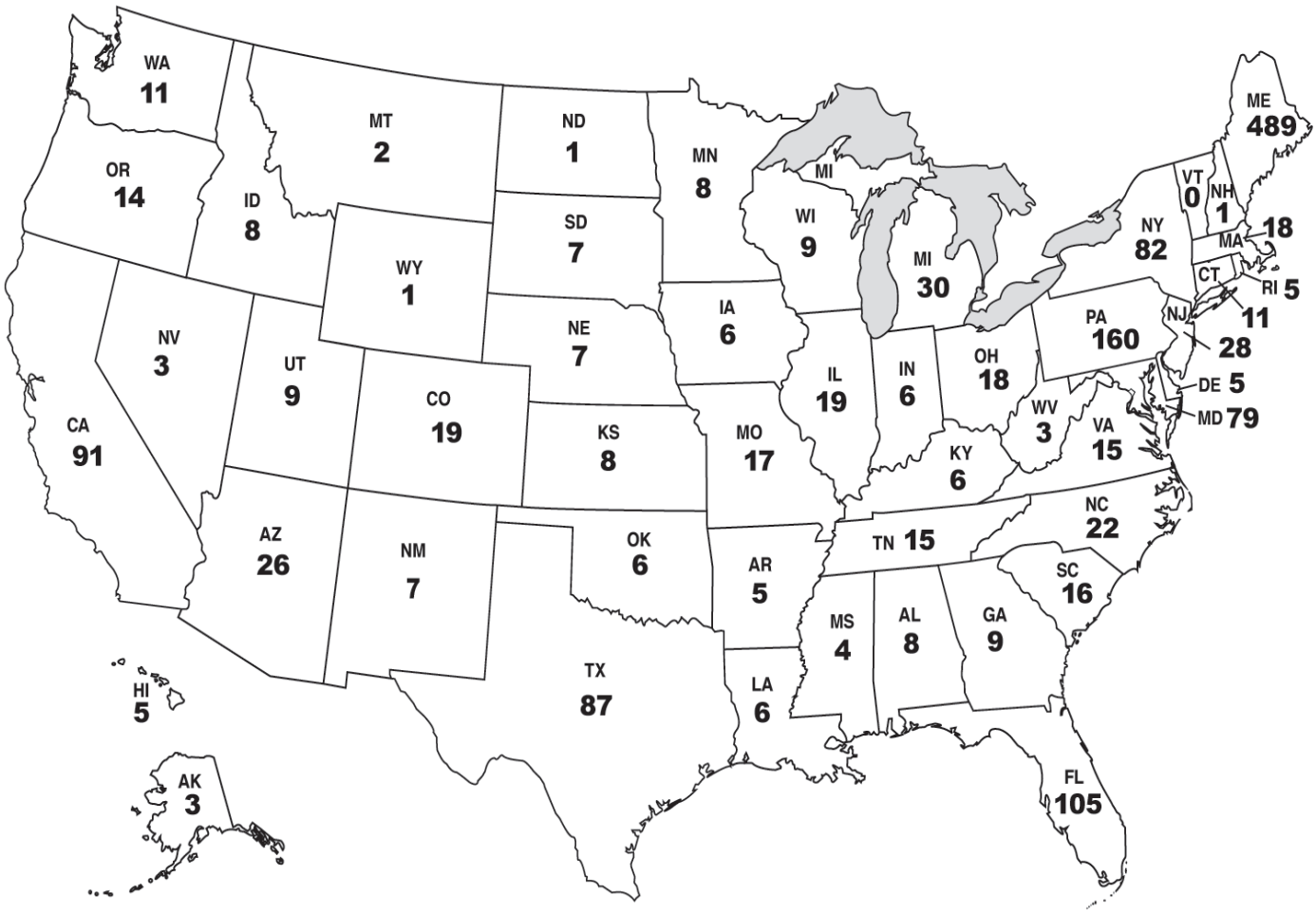
Robert P. Casey, Jr.
*Ranking Member*

# Top 10 Most-Reported Scams

From January 1, 2018, through December 31, 2018, the Senate Aging Committee's Fraud Hotline received a total of 1,509 complaints from residents all across the country. Calls pertaining to the top 10 scams featured in this report account for more than 65 percent of the complaints.

| Rank | Type of Scam | # of Complaints |
|---|---|---|
| 1 | IRS Impersonation Scam | 282 |
| 2 | Robocalls / Unsolicited Phone Calls | 149 |
| 3 | Sweepstakes Scam / Jamaican Lottery Scam | 99 |
| 4 | Computer Tech Support Scams | 82 |
| 5 | Elder Financial Abuse | 78 |
| 6 | Grandparent Scams | 71 |
| 7 | Romance Scams | 68 |
| 8 | Social Security Impersonation Scam | 64 |
| 9 | Impending Lawsuit Scams | 54 |
| 10 | Identity Theft | 45 |

# Origin of Calls Received by the Aging Committee Fraud Hotline



# Abbreviations

| | |
|---|---|
| Adult Protective Services | **APS** |
| Better Business Bureau | **BBB** |
| Department of Homeland Security | **DHS** |
| Department of Justice | **DOJ** |
| Federal Bureau of Investigation | **FBI** |
| Federal Communications Commission | **FCC** |
| Federal Trade Commission | **FTC** |
| Government Accountability Office | **GAO** |
| Health Insurance Claim Number | **HICN** |
| Internal Revenue Service | **IRS** |
| Internet Crime Complaint Center | **IC3** |
| National Adult Mistreatment Reporting System | **NAMRS** |
| Legal Services for the Elderly | **LSE** |
| Private Debt Collection | **PDC** |
| Social Security Administration | **SSA** |
| Social Security Number | **SSN** |
| Treasury Inspector General for Tax Administration | **TIGTA** |
| Voice over Internet Protocol | **VoIP** |

# Top Ten Types of Scams

## Reported to the Hotline


## 1 IRS Impersonation Scam

The Treasury Inspector General for Tax Administration (TIGTA) has called the Internal Revenue Service (IRS) impersonation scam "the largest, most pervasive impersonation scam in the history of the IRS."[1] According to TIGTA, more than 2.4 million Americans have been targeted by scammers impersonating IRS officials.[2] More than 14,700 Americans have lost a total of more than $72.8 million from this scam.[3] At the scam's peak, there were approximately between 20,000 and 40,000 people submitting complaints on this scam every week, with an average of 150 to 200 victims per week.[4] The IRS impersonation scam was the most frequent scam reported to the Committee's Fraud Hotline for the past four years.

In response to the initial flux of calls to the Fraud Hotline, the Committee held a hearing on April 15, 2015, titled, "*Catch Me If You Can: The IRS Impersonation Scam and the Government's Response*," that examined how the scam works, steps seniors can take to protect themselves, law enforcement's response, and what more can be done to combat this scam.[5] Since the hearing, the IRS has released several tips to spot these scams and what steps individuals should take if they receive a call.[6]

TIGTA data suggest that increased public awareness has made it more difficult for criminals to find victims.[7] TIGTA reports, however, that the scam has morphed and evolved in response to guidance the IRS has issued.[8] For example, one of the IRS's anti-fraud tips advises consumers that the agency will not call about taxes owed without first mailing a bill.[9] Recent fraud calls have revealed to investigators that some scam artists now claim that they are following up on letters that the IRS previously sent to the victims.


***Caller-ID Spoofing*** is a tactic used by scammers to disguise their true telephone numbers and or names on the victims' caller-ID displays to conceal their identity and convince the victims that they are calling from a certain organization or entity.

While there are multiple variations of the IRS impersonation scam, criminals generally accuse victims of owing back taxes and penalties. They then threaten retaliation, such as home foreclosure, arrest, and, in some cases, deportation if immediate payment is not made by certified check, credit card, electronic wire transfer, prepaid debit card or gift card. In April 2016, TIGTA announced that it began receiving an influx of complaints that IRS impersonators were demanding payment in the form of iTunes

gift cards.[10] At the same time, the Committee's Fraud Hotline also began receiving reports from callers that scammers were demanding payments via gift cards. The criminals tell victims that if they immediately pay the amount that is allegedly owed, the issue with IRS will be resolved and the arrest warrant, or other adverse action, will be canceled.

Once victims make an initial payment, they will often be told that further review of their tax records has identified another discrepancy and that they must pay an additional sum of money to resolve that difference or else face arrest or other adverse action. Scammers will often take victims through this process multiple times. As long as the victim remains hooked, the scammers will tell them they owe more money.

These scam calls most often involve a disguised, or "spoofed," caller identification (caller-ID) number to make the victim believe that the call is coming from the "202" area code, the area code for Washington, D.C., where the U.S. Department of the Treasury and the IRS are headquartered. In a recent variation of the scam, calls also appear to be coming from the "509," "206," and "306" area codes, all Washington State area codes. Scammers have also "spoofed" their phone numbers to make it appear as though they are calling from a local law enforcement agency when the unsuspecting victims see the "Internal Revenue Service" or the name of the local police department appear on their caller-IDs, they are understandably concerned and often willing to follow the supposed government official's instructions in order to resolve the alleged tax issue.

As of September 2018, a total of 130 individuals have been charged in federal court for their roles in the IRS impersonation scam.[11] According to TIGTA, 64 of those individuals have been sentenced and collectively received a total of more than 319 years' imprisonment.[12]

As a result of a tip reported to the Committee's Fraud Hotline, TIGTA was able, in May 2016, to arrest five individuals in Miami, Florida, connected with the IRS impersonation scam. Two individuals were identified as a direct result of the crucial information provided by a fraud investigator with the Committee's Hotline.[13] Based on the investigative results, in 2017, several additional suspects were identified as co-conspirators in this massive fraud scheme. TIGTA was ultimately able to identify and indict 10 additional suspects who were involved in the impersonation scam.[14] To date, the teams developed evidence and established that the 15 indicted individuals victimized nearly 8,000 people, stealing approximately $9,000,000 from the victims.[15]

**Fraud Case #1:**

"Scott" from Connecticut called the Fraud Hotline to report that his mother lost $120,000 to the IRS Impersonation Scam. Scott said someone claiming to work for the IRS called his mother and told her that her recently-deceased father owed a large debt to the IRS. The caller repeatedly demanded payments over the course of six months via electronic money transfers until the "debt" was paid. A Fraud Hotline investigator filed a report with TIGTA and the FTC.

The arrests stemmed from a call to the Aging Committee's Fraud Hotline in October 2015. The caller reported that an individual claiming to be from the IRS had recently contacted her husband demanding immediate payment of alleged back taxes. The scammer demanded that the victim drive to a local department store and wire nearly $2,000 via MoneyGram. On his way to the retailer, the distraught victim crashed his car. The victim was so convinced that the scammer was an authentic IRS agent, however, that he left the scene of the accident to wire the payment in order to avoid the scammer's threats of possible legal action.

The Fraud Hotline investigator who received the victim's report was able to trace the wire transfer to Minnesota and reported this information to TIGTA. TIGTA sent

agents to Minnesota, pulled surveillance tapes, and quickly identified three additional suspects.[16] Law enforcement arrested all five suspects and subsequently charged them with wire fraud and conspiracy to commit wire fraud.[17] At the time, this was the largest single law enforcement action in the history of the IRS impersonation scam.[18]

The largest enforcement action came on October 27, 2016, when TIGTA and DOJ announced that after an exhaustive, three-year joint investigation, 20 individuals were arrested in the United States and 32 individuals and five call centers in India were charged for their alleged involvement in the scam.[19] Following this crackdown, both TIGTA and the Committee's Hotline noticed a decline in the number of IRS scam cases being reported. During the scam's peak, TIGTA was receiving between 20,000 and 40,000 complaints a week, with an average of 150 to 200 victims a week. In December 2016, however, TIGTA reported receiving less than 2,000 calls a week, with fewer than 15 victims a week.[20] During the second week of January 2017, TIGTA reported that it received just eight new reports of victims losing money to this scam.[21] TIGTA believes this substantial drop-off is due, in part, to the October 2016 indictments of Indian call center operators.

**Fraud Case #2:**

"Randy" from Arizona called the Fraud Hotline to report that he had been contacted over the phone by a man claiming to work for the IRS. The caller alleged that Randy owed back taxes and would be arrested if he did not pay the IRS by the end of the day using gift cards. Fortunately, Randy did not believe the scammer and he refused to send money, at which point the scammer threatened to kill him and his children. Randy has no children, but was frightened by the threat. A Fraud Hotline investigator filed a report with TIGTA and the FTC.

The Committee's own data show that such arrests have a real impact. Prior to the October 2016 arrests, nearly three out of four calls to our Hotline involved the IRS impersonation scam. In the three months after the arrests, reports of the scam dropped an incredible 94 percent. Moreover, in 2017, the Committee saw an overall 77 percent reduction in the number of IRS impersonation scams reported compared to the previous year. On October 4, 2017, Genie Barton, the then President of the Better Business Bureau's Insitute for Marketplace Trust, testified before the Senate Aging Committee in a hearing titled *Still Ringing off the Hook: An Update on Efforts to Combat Robocalls* that her organization saw a similar trend. According to Ms. Barton, the Better Business Bureau's Scam Tracker saw an immediate 95 percent drop in reports of tax collection scams following the arrests.[22] Ms. Barton adds that while the volume of tax scams has since risen, the volume is only 30 percent of what of the scam's peak in 2016.

In addition to the arrests made in early 2017 in relation to the tip provided by the Senate Aging Committee, on September 4, 2018, TIGTA and the DOJ announced that 15 individuals and five call centers were indicted in

the Northern District of Georgia for their roles in the IRS impersonation scam that defrauded individuals out of more than $5.5 million.[23]

Beginning in April 2017, the IRS started doing something the taxpayers had been long told the IRS would never do – call taxpayers over the telephone to tell them they owe back taxes. A provision in the *Fixing America's Surface Transportation Act* (Pub. L. 114-94), passed by Congress in 2015, enabled the IRS to begin using private debt collectors (PDCs) to collect overdue tax debts. Under the new law, the IRS will first notify a taxpayer in writing that their account is being transferred to a private collection agency.[24] Once the IRS sends its letter, the private company will send its own letter and then may begin calling the taxpayer.[25]

While there have not yet been reports of fraudsters impersonating PDCs to scam delinquent taxpayers, TIGTA, the IRS, and consumer groups have expressed concerns that it may only be a matter of time before the scammers do so.[26] In response to concerns about the new PDC program and its possible susceptibility to scammers, Chairman Collins and Ranking Member Casey requested the Government Accountability Office (GAO) analyze the IRS's implementation of the PDC program. In particular, the senators asked GAO to compare the current program to lessons learned from previous times when the IRS used PDCs; how the IRS is tracking and comparing the costs and benefits of the PDC program; and how the IRS is protecting taxpayers from abusive PDC behavior as well from scams and identity theft, including protecting older Americans to ensure that the program does not increase the likelihood that they will be targeted by scam artists. The GAO has not yet completed the study.

### Fraud Case #3:

In February 2017, the Committee heard testimony from Philip Hatch, an 81-year-old resident of Portland, Maine, who lost $8,000 in the IRS scam and narrowly escaped losing another $15,000. Mr. Hatch paid the scammers using iTunes gift cards that he purchased at several different grocery and convenience stores. Mr. Hatch, who served 23 years in the Navy, described feeling both mad and upset that he had been scammed by these criminals.

**The IRS released the following tips to help taxpayers identify suspicious calls that may be associated with the IRS Impersonation Scam:**

- The IRS will never call a taxpayer to demand immediate payment, nor will the agency call about taxes owed without first having mailed a bill to the taxpayer.
- The IRS will never demand that a taxpayer pay taxes without giving him or her the opportunity to question or appeal the amount claimed to be owed.
- The IRS will never ask for a credit or debit card number over the phone.
- The IRS will never threaten to send local police or other law enforcement to have a taxpayer arrested.
- The IRS will never require a taxpayer to use a special payment method for taxes, such as a prepaid debit card or gift cards.

**Source:** *https://www.irs.gov/uac/Five-Easy-Ways-to-Spot-a-Scam-Phone-Call*

# 2 Robocalls and Unsolicited Phone Calls

In 2003, Congress passed legislation creating the national Do-Not-Call registry with the goal of putting an end to the plague of telemarketers who were interrupting Americans at all hours of the day with unwanted calls.[27] Unfortunately, 15 years after the registry was implemented, Americans are still being disturbed by telemarketers and scammers who ignore the Do-Not-Call registry and increasingly use robocall technology. According to the Federal Communications Commission (FCC), there are nearly 2.4 billion robocalls made every month.[28] To demonstrate the growing problem, in 2018, the Federal Trade Commission (FTC) received more than 3.8 million robocall complaints.[29] Robocalls help facilitate contact between scammers and potential victims.

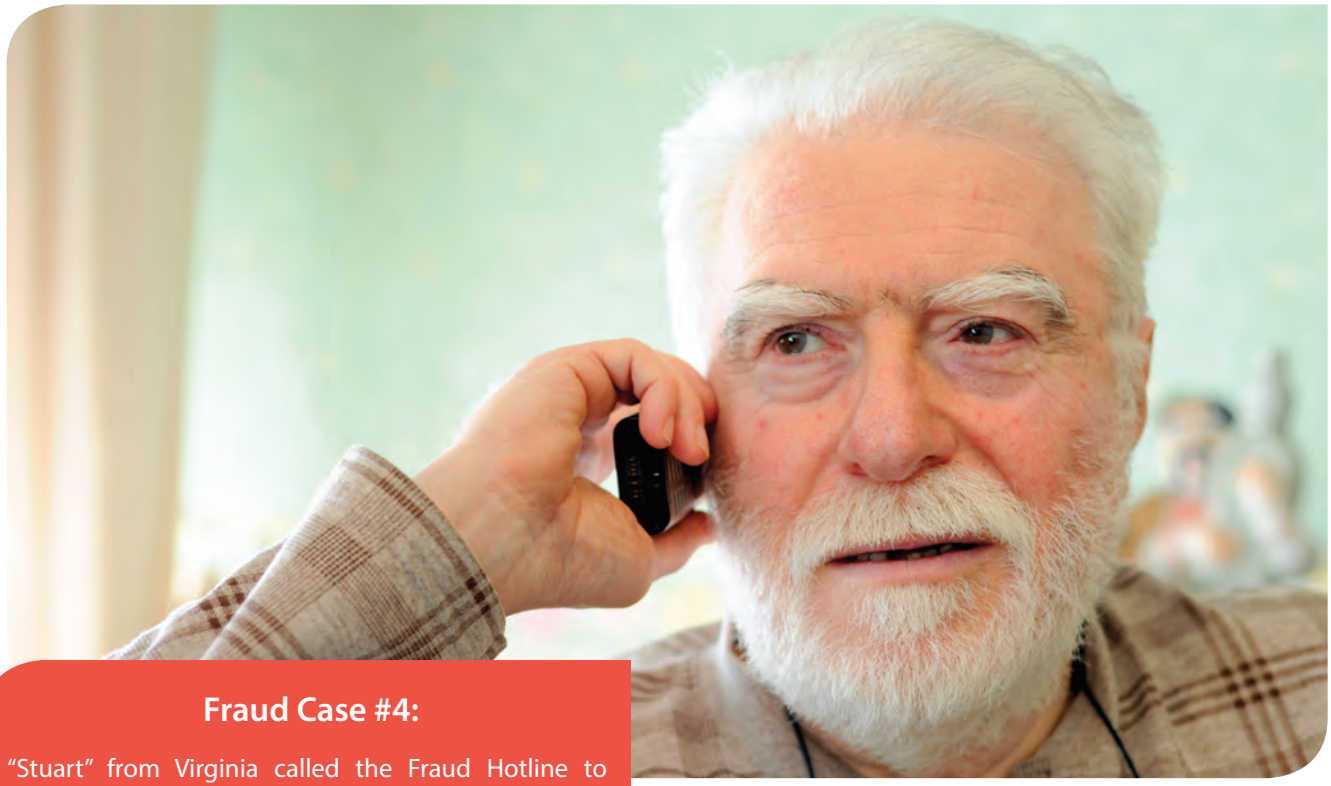
Robodialers can be used to distribute prerecorded messages or to connect the person who answers the call with a live person. Robocalls often originate overseas. Con artists usually spoof the number from which they are calling to either mask their true identity, or take on a new identity. As described in the first chapter on Internal Revenue Service impersonation scams, fraudsters spoof their numbers to make victims believe they are calling from the government or another legitimate entity. In addition, scammers are increasingly spoofing numbers to appear as if they are calling from the victims' home states or local area codes.

***Robocalling*** is the process of using equipment to mechanically, as opposed to manually, dial phone numbers in sequence.


Robocalls have become an increasing nuisance to consumers in recent years due to advances in technology. Phone calls used to be routed through equipment that was costly and made calling from international locations difficult and expensive. This traditional, or legacy, equipment sent calls in analog format over a copper wire network and could not easily spoof a caller-ID. Today, phone calls can be digitized and routed from anywhere in the world at virtually no cost. This is done using Voice over Internet Protocol (VoIP) technology, which sends voice communications over the Internet. Robocalling allows scammers to maximize the number of individuals and households they reach.

***Voice over Internet Protocol (VoIP)*** is a technology that allows a caller to make voice calls using a broadband Internet connections instead of a traditional (or analog) phone connection. Some VoIP services may only allow a user to call other people using the same service, but others may allow users to call anyone who has a telephone number, including local, long distance, mobile, and international numbers.

*Robocalls and Unsolicited Phone Calls*



**Fraud Case #4:**

"Stuart" from Virginia called the Fraud Hotline to report receiving a large number of telemarketing and soliciting phone calls, including some that were "obviously" scams. Stuart described calls about an expired warranty on his vehicle, even though his warranty was still current. A Fraud Hotline investigator advised Stuart to list his number on the national Do-Not-Call registry, and to contact his local telephone company and inquire about call blocking features.

Many companies now offer third-party spoofing and robodialing services. Third-party spoofing companies provide an easy-to-use computer interface or cell phone application that allows calls to be spoofed at a negligible cost. To demonstrate how accessible this technology is, an Aging Committee staff member spoofed two separate calls to Chairman Susan Collins during a Committee hearing on June 10, 2015, titled *Ringing Off the Hook: Examining the Proliferation of Unwanted Calls*."[30] By using an inexpensive smartphone app, the staff member was able to make it appear that the calls were from the Internal Revenue Service. The hearing examined why so many Americans are constantly receiving unsolicited calls even though they are on the national Do-Not-Call registry. The hearing also discussed how advanced in telephone technology makes it easier for scammers to cast a wide net to increase the number of potential victims they can reach, and highlighted possible technological solution for this menace.[31]

As Professor Henning Schulzrinne, a former FCC Chief Technology Officer, explained during the Committee's 2015 robocall hearing, it is possible to fight technology with technology, and the technology exists now for carriers to offer robocall filters that have proven effective in combatting robocalls. Previously, the primary impediment to carriers deploying robocall filters had been the concern that these filters violate the Commission's call completion requirements. In 2015, the FCC, under then-Chairman Wheeler, clarified that common carrier obligations do not restrict the ability of service providers to offer call-blocking technology to customers who request it.[32]

**Fraud Case #5:**

"Kate" from New York contacted the Fraud Hotline to report receiving unsolicited phone calls that display "Women's Cancer" on her caller-ID. The caller claims to offer help fighting breast cancer. Kate has repeatedly asked the caller to stop calling. The Fraud Hotline investigator filed a report with the FTC on her behalf. Kate was encouraged not to answer that call and other calls that she doesn't recognize on her caller-ID. In addition, Kate was advised to contact her local telephone company and inquire about call blocking features.

In 2016, the FCC convened a "Robocall Strike Force" comprised of telecom and tech company representatives to accelerate the development and adoption of new tools to combat illegal robocalls.[33] The Strike Force also seeks to promote greater consumer control over the calls they wish to receive, and to make recommendations to the FCC on the role government can play to stop these annoying calls. On October 4, 2017, Kevin Rupy, Vice President of Law and Policy at USTelecom, testified before the Aging Committee's hearing titled *Still Ringing Off the Hook: An Update on Efforts to Combat Robocalls* that the Strike Force has made significant progress toward arming consumers with call blocking tools and identifying ways voice providers can proactively block illegal robocalls before they ever reach the consumer's phone. The Strike Force has developed a blocking framework that includes four types of phone numbers to help increase flexibility given to voice providers to better block robocalls: invalid, unallocated, unassigned, and those requested by the subscriber.[34] On November 16, 2017, at the urging of Chairman Collins and Ranking Member Casey, the FCC took another step forward in protecting consumers from illegal robocalls.[35] The Commission voted to finalize new rules to allow phone companies to block certain phone numbers that do not or cannot make outgoing calls.[36] The rule allows providers to block numbers that are not valid under the North American Numbering Plan and block valid numbers that have not been allocated to any phone company. They are also able to block valid numbers that have been allocated to a phone number company but have not yet been assigned to a subscriber.

The new rule also codifies the FCC's previous guidance that phone companies can block calls when requested by the spoofed number's subscriber. For example, under the proposal, the IRS could request the blocking of its own numbers – including the public number (1-800-829-1040) taxpayers are instructed to call, but is never used to

make outgoing calls to taxpayers. That way, if someone attempts to spoof a number appearing to be the IRS's main line, it would be flagged as fraudulent and could be automatically blocked by the provider. This is precisely what Treasury Inspector General for Tax Administration (TIGTA), the Department of Homeland Security (DHS), and Verizon did in 2016 through a pilot program. Together, TIGTA, Verizon, and DHS blocked almost two million calls that were spoofed to appear as though the calls were being made from the aforementioned IRS phone number. The new rule gives providers the authority to block these calls and thus helps prevent countless seniors from falling victim to these scams by preventing these calls from getting to the senior in the first place.

In addition to the FCC, the FTC has also played a role in helping foster technological developments to combat robocalls. In response to the high volume of robocalls that are made in violation of the national Do-Not-Call Registry, the FTC launched a contest in October 2012 to identify innovative solutions to protect consumers from these calls.[37] In April 2013, the FTC announced that Nomorobo, a free service that screens and blocks robocalls made to VoIP phone numbers, was one of two winners of the Robocall Challenge.[38] Once a consumer registers his or her phone number, Nomorobo reroutes all incoming phone calls to a server that instantly checks the caller against a whitelist of legitimate callers and a blacklist of spammers.[39] If the caller is on the whitelist, the phone continues to ring, but if the number is on the blacklist, the call will disconnect after one ring. Aging Committee Fraud Hotline investigators have referred callers who contact the Hotline regarding robocalls to the Nomorobo website and have received positive feed back from callers who chose to register for the service.

In the spring of 2015, the FTC announced that it was launching two new robocall contest challenging the public to develop a crowdsourced "honeypot" and to better analyze data from an existing honeypot.[40] In this context, a honeypot is an information system that attracts robocalls so that researches can analyze them and develop preventive techniques.[41] In August 2015, the FTC announced that RoboKiller, a mobile app that blocks and forwards robocalls to a crowdsourced honeypot, was selected as the winner of the Robocalls: Humanity Strikes Back contests.[42] Champion Robosleuth, which analyzes data from an existing robocall honeypot and develops algorithms that identify likely robocalls, was selected as the winner of the FTC's DetectaRobo Challenge.[43]

**The Federal Communications Commission (FCC) has published the following tips for consumers to avoid being deceived by caller-ID spoofing:**

- Do not give out personal information in response to an incoming call. Identity thieves are clever: they often pose as representatives of banks, credit card companies, creditors, or government agencies to convince victims to reveal their account numbers, Social Security numbers, mothers' maiden names, passwords, and other identifying information.
- If you receive an inquiry from a company or government agency seeking personal information, do not provide it. Instead, hang up and call the phone number on your account statement, in the phonebook, or on the company's or government agency's website to find out if the entity that supposedly called you actually needs the requested information from you.

**Source:** *https://www.irs.gov/uac/Five-Easy-Ways-to-Spot-a-Scam-Phone-Call*


# 3 Sweepstakes Scams/ Jamaican Lottery Scams

Sweepstakes scams continue to claim senior victims 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 been entered to win a prize. Scammers then require the victims to pay a fee to either collect their supposed winnings or improve their odds of winning the prize.[44] According to the Federal Trade Commission (FTC), the number of sweepstakes scams increased by 45.8 percent between 2013 and 2017.[45,46] One example of such a scheme was reported in Pennsylvania by the *Lebanon Daily News*, which told of an 82-year-old man who lost $30,000 after paying "taxes" on $10.5 million in Publishers Clearing House "winnings."[47]

***Lead Lists*** are lists of victims and potential victims. Scammers buy and sell these lists and use them to target consumers in future scams.

During the 113th Congress, the Aging Committee launched an investigation of the Jamaican Lottery Scam, one of the most pervasive sweepstakes scams.[48] At its peak, law enforcement and FairPoint Communications estimated that sophisticated Jamaican con artists placed approximately 30,000 phone calls to the United States per day and stole $300 million per year from tens of thousands of seniors.[49]

Sweepstakes scams start with a simple phone call, often from a number beginning with "876," the country code for Jamaica. At first glance, this country code looks similar to a call coming from a toll-free American number. Scammers tell victims that they have won the Jamaican lottery or a brand new car, and that in order for their winnings to be delivered, they must first wire a few hundred dollars to cover processing fees and taxes. The criminals will often instruct their victims not to share the good news with anyone so that it will be a "surprise" when their families find out. Scammers tell victims to send money in a variety of ways, including prepaid debit card, electronic wire transfers, money orders and even cold hard cash.

Of course, no such winnings are ever delivered, and the "winners" get nothing but

**Fraud Case #6:**

"Michelle" called the Fraud Hotline to report that her parents, who live in Alabama, had lost $400,000 to the Jamaican Lottery Scam. They were told they had won hundreds of millions of dollars, but needed to send money to claim the "winnings." Over several month, the criminals convinced the couple to liquidate their assets, sell their house, and mail the money to the scammers. A Fraud Hotline investigator filed a report with the FTC and U.S. Postal Inspectors.

*Sweepstakes Scams/Jamaican Lottery Scam*

**Fraud Case #7:**

"Lisa" from New Mexico reported that criminals stole $300,000 from her mother-in-law. This began as a sweepstakes scam when a man called to tell her she had won a lottery. It evolved into a romance scam, and the caller began asking for money to help pay various expenses. The man eventually had the locks on her house changed, and her phone replaced remotely in order to cut her off from her concerned children. A Fraud Hotline investigator filed a report with the FTC and referred Lisa to state agencies and legal directories. The investigator also sent Lisa additional information on the sweepstakes and romance scams to share with her mother-in-law.

more phone calls, sometimes 50 to 100 calls per day, from scammers demanding additional money. Behind these calls is an organized and sophisticated criminal enterprise, overseeing boiler room operations in Jamaica. Indeed, money scammed from victims helps fund organized crime in that island nation.[50] Criminals once involved in narcotics trafficking have found these scams to be safer and more lucrative.

Since the Committee began investigating this issue, the Jamaican government passed new laws enabling extradition of the criminals to the United States for trial, leading to the extradition of one scammer for prosecution in the United States.[51] Several convictions have been obtained in connection with this scam. In November 2015, a 25-year-old Jamaican national living in the United States was sentenced to 20 years in prison after being found guilty of selling lists of potential victims referred to as "lead lists."[52]

Expensive "lead lists" identify potential victims. Satellite maps are used to locate and describe the victims' homes to make the callers appear familiar with the community. Elaborate networks for the transfer of funds are established to evade the anti-fraud systems of financial institutions. Should victims move or change their phone numbers, the con artists use all of the technology at their disposal to find them and re-establish contact. Fraud Hotline investigators have even heard reports of scammers calling the police to do wellness checks on victims, when they haven't heard from them in a couple of days.

While on a trip to Jamaica in early February 2018, then-Secretary of State Rex Tillerson noted the important progress Jamaica was making combating lottery scams, including cooperating closely with the United States to extradite suspected lottery scammers, and for establishing a bilateral lottery scam task force.[53] As Secretary Tillerson noted, it is in both countries' interests to work together to investigate crimes, share intelligence, conduct asset seizures where legal and appropriate to do so, and bolster existing anti-corruption and anti-gang programs.[54]

The con artists adopt a variety of identities to keep the money coming in ever-increasing amounts. Some spend hours on the phone convincing seniors that they care deeply for them. Victims who resist their entreaties begin receiving calls from Jamaicans 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.


# 4 Computer Tech Support Scams

The Aging Committee began seeing an increase in the frequency and severity of computer-based scams in 2015. Private industry has also seen a similar increase in the prevalence of this scam: Microsoft reported receiving more than 180,000 consumer complaints of computer-based fraud between May 2014 and October 2015.[55] The company estimated that 3.3 million Americans are victims of technical support scams annually, with losses of roughly $1.5 billion per year.[56] Unlike other victim-assisted frauds, where the scammers are successful in just one of a hundred-plus attempts, it appears that computer-based scams have a very high success rate.[57] In 2017, the Internet Crime Complaint Center (IC3), a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center, received 10,949 tech support fraud complaints with losses amounting to nearly $15 million.[58] The IC3 noted that while fraud affects victims of all ages, older victims are often the most vulnerable.[59]

In response to the increase in complaints to the Fraud Hotline, the Committee held a hearing on October 21, 2015 titled *Virtual Victims: When Computer Tech Support Becomes a Scam*.[60] The hearing featured representatives from Microsoft and the FTC who spoke about the challenges in combating this fraud given its many variations and constant changes.[61]

The basic scam involves 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 then falsely claim that the victims' computers have been infected with a virus. Con artists convince victims to give them remote access to their computers, personal information, and

### Fraud Case #8:

"Eileen" from Massachusetts called the Fraud Hotline to report that she had lost $400,000 over the course of two years to a tech support scam. She said her computer screen froze and displayed a message offering to fix the problem and protect her computer for $300. After paying, she was contacted and told that since she didn't use the service her $300 would be refunded, but only after she sent them $700 more because they could not send a check for less than $1,000. More requests for money followed, and she paid them all via gift card. Eileen eventually called the Fraud Hotline for advice, and an investigator reported the scammer to the FTC and the FBI's Internet Crime Complaint Center on her behalf. She was also eventually able to get the malware removed by the computer retailer.

*Computer Tech Support Scams*

credit card and bank account number so that victims can be "billed" for fraudulent services to fix the virus. In a related scam, individuals searching the internet may see a pop-up window on their computer instructing them to contact a tech-support agent. Sometimes, scammers have used the pop-up window to hack into victims' computers, lock them out, and require victims to pay a ransom to regain control of their computers.

Below are several of the most common variations of this scam:

- **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 "sponsored results." The FTC found that a network of scammers paid Google more than one million dollars since 2010 for advertisements for certain key search terms.[62] Some key search terms included: "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 fraudsters are associated with well-known companies. Other Fraudsters use pop-up messages on consumers' computer screens that direct potential victims to call them.

- **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 con artists usually direct the victims' computers to display benign error messages that appear on every computer to convince victims that their computers are malfunctioning. Scammers generally charge victims between $150 and $800 and may install free programs or trial versions of antivirus programs to give the illusion that they are repairing victims' computers. If victims express concern about the price, the con artists will often entice victims to pay by offering a "senior citizen discount."
- **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, however, the fraudsters use the victims' account information to charge consumers.
- **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, prompting the appearance of a blue screen that can only be removed with a password known by the scammers. The Fraud Hotline has received reports that scammers sometimes admit to victims that it is a scam and refuse to unlock the victims' computers unless a "ransom" payment is made.

### Fraud Case #9:

"Arlene" from California reported that she was targeted by a computer scam. She clicked on a pop-up advertising IT support services for one year for $300. She paid and thought she had subscribed to the service. After five months, she received a series of calls offering her a refund because, the caller said, she had not used the service. However, they required her to give her private bank information in order to receive the refund. She gave them some of the information before she realized this was a scam. She eventually realized that her computer had been taken over remotely and infected with malware. She contacted her bank to protect her account and had her computer cleaned by the retailer. A Fraud Hotline investigator reported this to the FTC and the FBI's Internet Crime Complaint Center.

The FTC has responded to computer-based scams through law enforcement actions and ongoing investigations. In 2014, the agency brought actions against six firms based primarily in India that were responsible for stealing more than $100 million from thousands of victims.[63]

On May 12, 2017, the Department of Justice (DOJ) announced that seven individuals were charged for their participation in the tech support scam.[64] Seven individuals received criminal indictments for their role in the Florida-based Client Care Expert Fraudulent operation. According to the indictments, Client Care/First Choice purchased pop-up advertisements, which appeared without warning on the victims' computer screens and locked up their browsers.[65] These pop-ups falsely informed the victims that serious problems, such as viruses or malware, had been detected on their computers.[66] From approximately November 2013 through 2016, Client Care Experts victimized over 40,000 people and defrauded these individuals out of more than $25,000,000.[67]

In May 2018, three individuals were charged in the Southern District of Illinois for allegedly operating two tech support scam businesses.[68] According to the DOJ, the defendants purchased pop-up advertisements, which appeared without warning on consumers' computer screens and locked up their browsers.[69] These pop-ups falsely informed the victims that serious problems, such as viruses or malware, had been detected on their computers. Once they had accessed the victims' computers, the indictments charge, the salespersons examined routine computer functions and processes and then tried to convince the victims that these functions and processes were evidence of problems.[70]

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

- Do not give control of your computer to a third party that calls you out of the blue.
- Do not rely on caller ID to authenticate a caller. Criminals spoof caller ID numbers. They may appear to be calling from a legitimate company or a local number when they are not even in the same country as you.
- If you want to contact tech support, look for a company's contact information on its software package or on your receipt. Never provide your credit card or financial information to someone who calls and claims to be from tech support.
- If a caller pressures you to buy a computer security product or says there is a subscription fee associated with the call, hang up.
- If you're concerned about your computer, call your security software company directly and ask for help.
- Make sure you have updated all of your computer's anti-virus software, firewalls, and popup blockers.

# 5 Elder Financial Abuse

Financial exploitation of older Americans is the illegal or improper use of an older adults fund's property, or assets. According to the Government Accountability Office (GAO), seniors lose an estimated $2.9 billion annually due to financial exploitation, although these numbers are likely substantially underreported.[71] A 2011 GAO study found that approximately 14.1 percent of adults age 60 and older had experienced physical, psychological, or sexual abuse; potential neglect; or financial exploitation in the previous year.[72]

The Fraud Hotline documents complaints of elder abuse and refers calls to local jurisdiction's Adult Protective Services (APS) for further action. APS employees receive reports of alleged abuse, investigate these allegations, determine whether the alleged abuse can be substantiated, or arrange for services to ensure victims' well-being.[73] APS can also refer cases to law enforcement agencies or district attorneys for criminal investigation and prosecution.[74] APS workers ideally coordinate with local law enforcement and prosecutors to take legal action, but the effectiveness of this relationship can vary significantly from state to state. As of 2015, every state has an elder abuse statute.[75]

Older Americans are particularly vulnerable to financial exploitation because financial decision-making ability can decrease with age. One study found that women are almost twice as likely to be victims of financial abuse.[76] Most victims are between the ages of 80 and 89, live alone, and require support with daily activities.[77] Perpetrators include family members, paid homecare workers, those with fiduciary responsibilities (such as financial advisors or legal guardians), or strangers who defraud older adults through mail, telephone, or Internet scams.[78]

Victims whose assets were taken by family members typically do not want their relatives to be criminally prosecuted, leaving civil actions as the only mechanism to recover stolen assets.[79] Few civil attorneys, however, are trained in issues related to older victims and financial exploitation.[80] Money that is stolen is rarely recovered, which can undermine victims' ability to support or care for themselves. Consequently, the burden of caring for exploited older adults may fall to various state and federal programs.[81]

One of the provisions of the Elder Justice Act of 2009, which was enacted in 2010, formed the Elder Justice Coordinating Council, which first convened on October 11, 2012. The Council is tasked with increasing cooperation among federal agencies.[82] Experts agree that multidisciplinary teams that bring together professionals from various fields such as social work, medicine, law, nursing, and the financial industry can expedite and resolve complex cases, identify systemic problems, and raise awareness about emerging scams.[83]

The *Elder Abuse Prevention and Prosecution Act* (Pub.L. 115-70), signed into law on October 18, 2017, and co-sponsored by Aging Committee Chairman Collins and Ranking Member Casey further improves the federal response to the issue of elder abuse. The law compels the Department of Justice (DOJ) and FTC to designate Elder Justice Coordinators in each federal district to oversee activities relating to elder justice and evaluate best practices for the DOJ, FTC, other federal agencies, and state agencies for preventing and prosecuting elder financial abuse.[84]

**Fraud Case #10:**

"Sandra" from Florida called the Fraud Hotline to report that she was defrauded by her neighbor and supposed friend. The neighbor pretended to take an interest in Sandra's welfare and convinced her to loan the neighbor's daughter $400. The money was not repaid. The neighbor then got involved in Sandra's banking and convinced her to withdraw $1,200 from the bank to keep in a safe. Instead, the neighbor allegedly stole the money, and then drained Sandra's bank account. A credit card and bank account were later fraudulently established in her name. A Fraud Hotline investigator reported this to the Florida APS, local police, and sheriff, and advised Sandra through the process of recovering her identity.

While some states have laws that require financial professionals to report suspected financial exploitation of seniors to the appropriate local or state authorities, there currently is no federal requirement to do so. Some financial professionals may fail to report suspected financial exploitation due to a lack of training or fear of repercussions for violating privacy laws. Chairman Collins and former Ranking Member Claire McCaskill authored the Senior$afe Act, a bipartisan bill cosponsored by Ranking Member Casey and others, which would provide certain individuals with immunity for disclosing suspected financial exploitation of senior citizens.[85] The Senior$afe Act was signed into law on May 24, 2018 as part of the *Economic Growth, Regulatory Relief, and Consumer Protection Act* (Pub.L. 115-174).

Some localities with large senior populations have established special units to address all forms of elder abuse, including elder financial abuse. In October 2015, prosecutors in Montgomery County, Maryland, successfully brought charges against an individual who, over several years, embezzled more than $400,000 before one of the victims' bankers discovered suspicious activity in his account and alerted APS.[86] The fraudster had convinced the victim to give her power of attorney and control of his finances. She was sentenced to five years in jail for financial exploitation of a vulnerable adult, theft, and embezzlement.[87]

In March 2016, an attorney in Belfast, Maine, was sentenced to 30 months in prison for bilking two elderly female clients out of nearly half of a million dollars over the course of several years.[88] The lawyer's brazen theft was uncovered when a teller at a local bank noticed that he was writing large checks to himself on his clients' accounts.[89] When confronted by authorities, he offered excuses that the prosecutor later described as "breathtaking."[90] For example, according to the *Bangor Daily News*, the local paper of Bangor, Maine, he put one of his clients in a nursing home to recover from a temporary medical condition, and then kept her there for four years until the theft of her

funds came to light. Meanwhile, he submitted bills for "services," sometimes totaling $20,000 a month, including charging her $250 per hour for six to seven hours to check on her house, even though his office was just a one-minute drive down the road.[91]

Another tragic case of theft and abuse was featured in a November 2016 *Maine Sunday Telegram* article. The article detailed the story of an elderly woman from Los Angeles, California, who went missing in 2008.[92] In 2012, authorities found her, alive but in poor health, abandoned in a tiny cabin in Maine by three people who had "befriended" her years earlier. After gaining the woman's trust and control of her finances, these criminals sold her house and stole her money, cheating her of an estimated $1 million in assets.[93] Today, this 90-year-old woman is a ward of the state and lives in a nursing home in rural Maine – thousands of miles away from the life she used to know.[94]

The Aging Committee has brought to light many schemes that have defrauded seniors out of their hard-earned retirement savings. It is deeply troubling when a senior falls victim to one of these schemes, but it's even more egregious when the perpetrator is a family member, caregiver, or trusted financial advisory.

In November 2016, the Aging Committee examined financial abuse committed by guardians and other court-appointed fiduciaries in a hearing titled *Trust Betrayed: Financial Abuse of Older Americans by Guardians and Others in Power.* The Committee released a GAO report on guardianship abuse that found hundreds of cases of abuse, neglect, and exploitation that improperly diverted over $5 million. The report concluded that abuse is widespread, but it remains difficult to determine the extent of elder abuse by guardians nationally due to limited data.[95]

Some progress is being made to collect data on guardianships and improve the guardianship process. In 2013, the Department of Health and Human Services (HHS) began

developing the National Adult Mistreatment Reporting System (NAMRS) to provide consistent and accurate national data on senior abuse. HHS completed the pilot project in 2015 and issued its first report in August 2017.

In addition, GAO identified a number of measures that can be taken to protect seniors from guardianship abuse, including for courts to ensure that a guardianship is truly needed before appointing one and periodically reexamining whether a guardianship is still needed. Courts should also make sure that guardians are screened for criminal backgrounds and are properly educated on their role and responsibilities.

During the hearing, the Committee heard testimony about some of the promising initiatives that are being undertaken at the state level to combat this form of financial exploitation. One such example is the Minnesota Conservator Account Auditing program, which monitors guardians of seniors by requiring them to file regular reports. The state uses an automated, software-based system that scans these conservator reports for 30 "red flags" that may indicate abuse or mismanagement of the estate. Minnesota is making this innovative software reporting and analysis available to other states free of charge.

Another witness, Jaye Martin, the Executive Director of Legal Services for the Elderly (LSE) in Maine, testified that her organization assisted 260 victims of elder abuse in 2016. This was a 24 percent increase from the prior year. While this number includes physical and emotional abuse as well, roughly half of the cases handled by the LSE involved financial exploitation of seniors. Even more alarming was Ms. Martin's testimony that in 75 percent of those cases, the financial exploitation was carried out by a family member. Unfortunately, these numbers may only represent the tip of the iceberg, since so many abuse cases go unreported. Victims are often ashamed or afraid to alert authorities about financial exploitation, particularly when it involves a family member.

In 2018, the Committee was again alerted to appalling stories from Americans across the country regarding abusive guardianships that take advantage of vulnerable individuals. The Committee launched a year-long examination of ways in which the guardianship system can be improved to better protect individuals subject to these and similar arrangements from abuse, neglect, and exploitation. The Committee held two hearings and issued a report in November titled, "*Ensuring Trust: Strengthening State Efforts to Overhaul the Guardianship Process and Protect Older Americans."* As a result of the Committee's work, Chairman Collins and Ranking Member Casey introduced the *Guardianship Accountability Act.* This bipartisan legislation would promote information sharing among courts and local organizations as well as state and federal entities, encourage the use of background checks and less restrictive alternatives to guardianship, and expand the availability of federal grants to improve the guardianship system.

# 6 Grandparent Scams

A common scam that deliberately targets older Americans is the "grandparent scam." In this scam, imposters either pretend to be the victims' grandchild and/or claim to be holding the victims' grandchild. The fraudsters claim that 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 victims' emotions and trick concerned grandparents into wiring money to them. For example, in 2017, the *Lebanon Daily News* in Pennsylvania reported a grandmother being scammed out of thousands of dollars after being told her granddaughter had been arrested and jailed.[96]

**Fraud Case #11:**

"Susan" from Connecticut called the Fraud Hotline to say that her parents received a call from an "attorney" who claimed that their daughter was to blame for a deadly car accident and that she was being held in jail on $8,500 bail. Susan's parents were instructed to FedEx cash to an address in New York. Fortunately, Susan happened to call her parents that same day and they realized this was a scam. They canceled the FedEx in time to recover their money. A Fraud Hotline investigator reported the address of the FedEx recipient to the FTC to begin the investigation.

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 in hopes the scam won't be uncovered. Recently, the Fraud Hotline has received reports of imposter grandchildren claiming to have broken their noses to explain why their voices sound differently. The scammer then asks the victim to help by sending money in the fastest way possible. This typically requires the victim to go to a local retailer and send an electric wire transfer of several thousand dollars.

After payment has been made, the fraudster will more likely than not call the victim back, claiming that there was another legal fee of which they were not initially aware. In 2018, for example, the Fraud Hotline received multiple reports of scammers initially claiming to have been in a car accident and requesting bail, then calling back and claiming that a pregnant woman was in the other car and suffered a miscarriage as a result of the accident. They then begged for thousands of dollars to retain a lawyer or pay the woman off so they could avoid going to court. The second call is typically what alerts the victims that they have been scammed. Victims have told Fraud Hotline investigators that once they realized they had been duped, they wished that they had asked the con artist some simple questions that only their true grandchild would know how to answer.

*Grandparent Scams*

### Fraud Case #12:

"Timothy" from Pennsylvania called to report losing $40,000 in a grandparent scam. He was called by someone impersonating his grandson who asked for money to help with repairs to his car after an accident. This went on for a month, with the "grandson" calling and continually asking for help with legal fees and repairs, until Timothy had lost $40,000 and realized that this was a scam. A Fraud Hotline investigator filed a report with the FTC on his behalf and sent him a copy of the Fraud Book.

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 con artist impersonating victims' grandchildren to talk briefly with the victims and then hand the phone over to an accomplice impersonating an authority figure. This gives the scammers' stories more credibility and reduces the chance that the victim will recognize that the voice on the phone does not belong to their grandchild.

In 2017, the Federal Trade Commission (FTC) received 18,912 complaints of individuals impersonating friends and family members, up from 12,404 in 2013.[97], [98] Between January 1, 2012, and May 31, 2014, individuals reported more than $42 million in losses to the FTC from scams involving the impersonation of family members and friends.[99]

In March 2018, six defendants were sentenced in the Northern District of Iowa in connection with their participation in the grandparent scam. In total, the defendants defrauded more than 250 victims of more than $750,000.[100] The defendants, who pled guilty in October and November of 2017, each admitted that other individuals called victims on the phone and falsely claimed that relative was in jail.[101] The caller asked the victims to wire money via Western Union or MoneyGram to secure the relative's release.[102] The defendants were sentence to prison terms ranging from eight months to 33 months and were ordered to pay restitution.[103]

### Fraud Case #13:


In March 2018, Stephen and Rita Shiman, from Maine, testified at an Aging Committee hearing on phone scams. Stephen and Rita were called in May 2015 by someone who said he was their grandson, Kabo. Rita said the caller's voice sounded just like that of her grandson. He claimed that he was being held in a county jail in Georgia. When Rita asked why he was in Georgia and not home in Maryland, he answered that a classmate from college had died and he drove with several friends for the funeral. "Kabo" made Rita promise not to tell his parents (the Shimans' son and his wife) about this and told her a public defender would be calling soon to arrange bail. A man calling himself George Diaz called soon after and told them that he was meeting with the judge shortly and needed them to send $1,230 as quickly as they could to secure Kabo's release. He said the transaction would have to be in cash sent via Western Union to his contact in the Dominican Republic. Stephen and Rita described feeling so panicked by the situation that they did not think twice about the strange instructions. He said that Western Union had no legal right to question the transaction and advised them not to answer any questions if an employee did so. Only after sending the money and returning home did Stephen and Rita begin to realize that the instructions were quite suspicious. After they received a second call from the defender telling them the first amount of money was not sufficient and they would need to send more, they called their son's home phone number in Maryland and Kabo picked up. They realized they had been scammed.


# 7 Romance Scams

More and more Americans are turning to the Internet for dating. As of February 2016, approximately 15 percent of American adults had used online dating services.[104] In particular, online dating use among seniors has also risen in recent years. According to the Pew Research Center, 12 percent of those aged 55- to 64-years-old reported using an online dating site or mobile dating app. This is an increase from just six percent in 2013.[105]

As Americans increasingly turn to online dating to find love, con artists are following suit — not for love, but for money. In 2014, the Aging Committee's Fraud Hotline began receiving reports from individuals regarding romance scams, with the number of reports increasing each year. Sometimes these reports were not just from seniors, but also from friends and family members whose loved ones were deeply involved in a fictitious cyber-relationship. This is one of the most heartbreaking scams because con artists exploit seniors' loneliness and vulnerability.

In a related scam known as confidence fraud, con artists gain the trust of the victim by assuming the identities of U.S. soldiers. Victims believe they are corresponding with an American soldier who is serving overseas who claims to need financial assistance. Scammers will often take the true name and rank of a U.S. soldier who is honorably serving his or her country somewhere in the world, or has previously served and been honorably discharged. In addition, the con artist will even use real photos of that soldier in their profile pages, giving their stories more credibility.

Typically, scammers contact victims online either through a chatroom, dating site,

**Fraud Case #14:**

"Gail" from Tennessee called the Fraud Hotline to report that she was the victim of a romance scam. A man contacted her via the online game, "Words with Friends," and they developed a romantic relationship. The man told her that he has $12 million in gold and works on an oil rig in Nigeria, but needed her help to access it. Gail had sent the man $500,000 and depleted her retirement account before she realized that this was a scam. A Fraud Hotline investigator filed a report with the FTC and IC3 on her behalf, and also sent her a copy of the Fraud Book to help her understand how else she may be targeted by him.

social media site, or email. According to the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3), 90 percent of the complaints submitted in 2016 contained a social media aspect.[106] Con artists have been known to create elaborate profile pages, giving their fabricated story more credibility. Con artists often call and chat on the phone to prove that they are real. These conversations can take place over weeks and even months as the con artists build trust with their victims. In some instances, con artists have even promised to marry their victims.

Inevitably, con artists in these scams will ask their victims for money for a variety of things. Often, con artists will ask for travel expenses so they can visit the victims in the United States. In other cases, they claim to need money for medical emergencies, hotel expenses, hospital bills for a child or relative, visas or other official documents, or losses from a temporary financial setback.[107] Unfortunately, in spite of telling their victims they will never ask for any more money, something always comes up resulting in the con artist requesting more money.

Con artists may send checks for victims to cash under the guise that they are outside the country and cannot cash the checks themselves, or they may ask victims to forward the scammer a package. The FBI warns that, in addition to losing money to these con artists, victims may also have unknowingly taken part in money laundering schemes or shipped stolen merchandise.[108]

In 2017, the FBI's IC3 received 15,372 complaints about romance and confidence scams that cost victims $211,382,989, the second highest type of scam by victim loss reported to the IC3.[109] In comparison, in 2014, the IC3 receiving 5,883 complaints about romance and confidence scams that cost victims $86.7 million.[110] Nearly half of the victims in 2014 were age 50 or older, and this group accounted for approximately 70 percent of the money lost to this scam in 2016.[111] Romance and confidence scams disproportionately target women, usually between the ages of 30 and 55 years old.[112] Unfortunately, both the amount of financial loss and the number of complaints for the crime have increased in recent years.[113] One study found that, for every case of financial fraud that is reported as many as 14 go unreported.[114]

**Tips from the FBI's Internet Crime Complaint Center to help prevent consumers from falling victim to romance scams:**

- Be cautious of individuals who claim the romance was destiny or fate, or that you are meant to be together.
- Be cautious if an individual tells you he or she is in love with you and cannot live without you but needs you to send money to fund a visit.
- Fraudsters typically claim to be originally from the United States (or your local region), but are currently overseas, or going overseas, for business or family matters.

**Source:** *https://www.fbi.gov/news/news_blog/2014-ic3-annual-report*


# 8 Social Security Impersonation Scam

A new scam to make the top 10 list for 2018 involves consumers receiving calls from individuals claiming to represent the Social Security Administration (SSA). While there are several variations of this scam, the caller generally asks for personal information such as Social Security number, date of birth, mother's maiden name, and/or bank or financial account information.

Scammers are out to do so Social Security numbers and will go to great lengths to obtain it. Scammers will try to get your information by offering to help complete a disability application, apply for a piece of medical equipment, or obtain a new Medicare card.

It is important to note that according to SSA, SSA employees occasionally reach out by telephone for customer-service purposes.[115] In only a few special situations, usually already known to the individual, an SSA employee may request the confirmation of personal information over the phone. SSA warns that true SSA callers will provide a telephone number and extension.

In addition to phone calls, some people have reported getting emails claiming to be from SSA. According to SSA's website, "Social Security will not send you an email asking you to give us your personal information, such as your Social Security number, date of birth, or other private information. If someone saying they are from Social Security does email you requesting information, don't respond to the message."[116]

### Fraud Case #15:

"John" from Tennessee called the Fraud Hotline to report that he received a robocall from someone claiming to work for the Social Security Administration, who alleged there had been fraudulent activity on his account. John returned the call, and the man who answered tried to convince John to reveal his Social Security number. John knew this was a scam and he called the Fraud Hotline. An investigator filed a report with the FTC and the SSA OIG.

### Tips to Help Secure Your Identity:

- Social Security will not call to ask for your bank account information or SSN.
- There will never be a fee charged to obtain a Social Security card.
- Social Security numbers do not get suspended.
- Never give out personal information over the phone to someone you do not know.
- Don't be afraid to call SSA's Inspector General at their toll free number (1-800-772-1213) to verify the caller/request.


# 9 Impending Lawsuit Scams

In 2018, for the first time, the Impending Lawsuit Scam entered the top ten of most-reported scams to the Committee's Fraud Hotline. We received 54 complaints of this scam in 2018, a 32 percent increase over 2017.

Similar to the IRS Impersonation or Social Security Impersonation scams, the Impending Lawsuit Scam typically involves consumers receiving calls from individuals claiming to be from local, state, or federal law enforcement agencies. Consumers are told that there is a warrant out for their arrest, and unless the person agrees to pay a fine, they will be immediately arrested. Often times, the caller says the arrest warrant was issued for failing to report for jury duty. To give the calls more credibility, scammers will often spoof their call so caller-ID appears to show that the call is coming from a local sheriff's or police department.

**Fraud Case #16:**

"Sally" from Maine called the Fraud Hotline to report receiving a call from someone named Deputy Davis claiming to be with the Kennebec County Sheriff's Department. The caller told her she had missed jury duty and she faced legal action. Sally said the call was to her business and not her home. Although the caller-ID displayed "Kennebec County Sheriff's Office," Sally suspected it was a scam and hung up. A Fraud Hotline investigator reported the call to the Sheriff's Office and the FTC.

Usually, the caller imposes a deadline, such as the end of the business day, by which the police will come for the victim for ignoring court summonses. In these scams, no such summonses have been issued, but scammers will try to convince their victim that multiple notices have been sent that they have missed. The scammer then either asks for payment to resolve the issue without arresting the victim, or for personal information, such as a Social Security number, that could compromise their identity. While scammers usually create a sense of urgency or attempt to fluster the victims, some variations have scammers calmly asking for personal information as a matter of procedure to then sell to identity thieves.

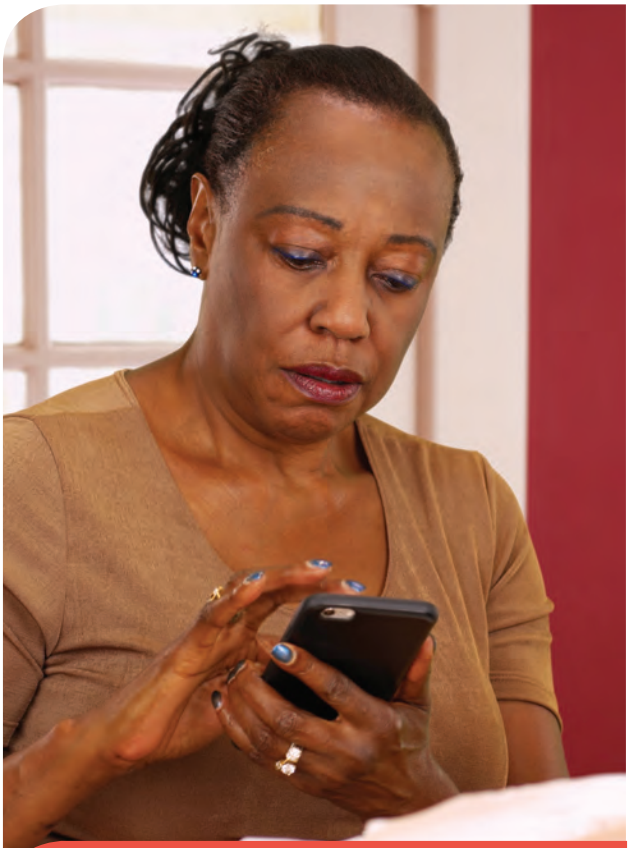
As the Committee learned in the IRS Impersonation Scam, lawsuits were often the threatened penalty for non-payment of taxes, and Fraud Hotline investigators noticed a gradual shift from scammers threatening arrest for non-payment of taxes to threatening lawsuits, or dropping the IRS impersonation altogether and just threatening lawsuits. With greater awareness of the IRS Impersonation Scam, scammers seem to be turning to the Impending Lawsuit Scam as an alternative.

In one variation of this scam, the Committee has heard stories of immigrant communities being targeted by scammers who allege the potential victim has errors in their immigration paperwork and faces immediate deportation. In lieu of arrest and deportation, potential victims are told to pay a fee.

# 10 Identity Theft

Identity thieves not only disrupt the lives of individuals by draining bank accounts, making unauthorized credit card charges, and damaging credit reports, but they also often 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. Fraudsters also use stolen personal information, including Social Security numbers (SSN), to commit tax fraud or to fraudulently apply for jobs and earn wages. According to the Federal Trade Commission (FTC), identity theft was the second-most common type of consumer complaint in 2017, with 371,061 complaints.[117] Consumers aged 50 and older reported 37 percent of the identity theft complaints that the FTC received in 2017.[118]

The growing use of commercial tax filing software and online tax filing services has led to opportunities for thieves to commit fraud without stealing SSNs. In some cases, thieves can illegally access an existing customer's account simply by entering that individual's username, email address, or name and correctly-guessed password. This is often referred to as an "account takeover." Whether the thief uses this method to access an existing account or uses stolen personal information to create a new account, the end result is often the same: early in the tax filing season, the thief files a false tax return using a victim's identity and directs the refund to his own mailing address or bank account. The victim only discovers this theft when they files their own return and the Internal Revenue Service (IRS) refuses to accept it because a refund has already been issued. In November 2015, the IRS reversed a long-standing policy and now provides victims



### Fraud Case #17:

"Barbara" from Michigan called the Fraud Hotline to report that she tried to open a utility account and found that her credit score had precipitously declined. She then received a bill in the mail for insurance on a car she did not own. It seemed that someone had stolen her identity and opened a credit card in her name. A Fraud Hotline investigator referred her to IdentityTheft.gov and advised her on communicating with her bank, credit card companies, and credit rating agencies to secure her finances. The investigator also sent her a Fraud Book with more information.

with copies of the fake return upon written request.[119] The documents will provide victims with details to help them discover how much of their personal information was stolen. The IRS saw a marked improvement in the battle against identity theft in 2017.[120] According to the IRS, the number of people reporting stolen identities on federal tax returns fell by more than 40 percent, with 242,000 fewer victims compared to a 2016.[121]

Medical identity theft occurs when someone steals personal information – an individual's name, SSN, or health insurance claim number (HICN) – to obtain medical care, buy prescription drugs, or submit fake billings to Medicare. Medical identity theft can disrupt lives damage credit ratings, and waste taxpayer dollars. Some identity thieves can even use stolen personal information to obtain medical care for themselves or others, putting lives at risk if the theft is not detected and the wrong information ends up in the victims' medical files. Claims for services or items obtained with stolen HICNs may be included in the beneficiary's Medicare billing history and can delay or prevent the beneficiary from receiving needed services until the discrepancy is resolved.

In April 2015, President Obama signed a law that requires the Centers for Medicare & Medicaid Services (CMS) to remove SSNs from Medicare cards by 2019.[122] Medicare began mailing new Medicare cards to beneficiaries in April 2018.[123] On October 7, 2015, the Aging Committee held a hearing titled *Protecting Seniors from Identity Theft: Is the Federal Government Doing Enough?*.[124] The Committee heard testimony from the CMS official in charge of implementing the Medicare card replacement process and from the Department of Health and Human Services Office of Inspector General about investigative efforts to combat medical identity theft.[125]

The 2017 Equifax data breach may have exposed private information belonging to 145.5 million people – nearly half the U.S. population.[126] The Senate Aging Committee

### Fraud Case #18:

"James" from North Carolina called the Fraud Hotline to report that his mother passed away in January 2016. Since June of that year, someone has been using her identity on credit cards and car loans. James was not made aware of this until the credit company contacted him in 2017. The Fraud Hotline investigator sent him the identitytheft.gov link and a Fraud Book for more information. The investigator also encouraged him to work with the credit card company and credit reporting agencies.

was particularly concerned with the devastating impact this breach could have on older Americans, whose retirement savings and financial security are at unique risk. In the aftermath of this data breach, Chairman Collins and Ranking Member Casey sent a letter to Equifax seeking additional information on the steps the company has taken and plans to take in an effort to mitigate and remediate the unique threats facing seniors, including risks for their life savings, entitlement benefits, and credit scores.

Scammers have begun capitalizing on the breach through robocalls claiming to be calling from Equifax to verify account information.[127] The scammers try to trick victims into sharing personal identifiable information, such as their Social Security numbers. In a case reported to the Better Business Bureau's Scam tracker on September 15, 2017, a consumer in New Jersey reported receiving a voicemail from someone claiming to be from the IRS saying that a lawsuit had been filed against the consumer for unpaid back taxes. When the consumer called the number left in the voicemail, the consumer was told that his information had been compromised in the Equifax security breach, and that the consumer would have to pay $100,000 in back taxes.[128] The scammer also tried to get the consumer's sensitive personal information, including full name and SSN.

### Tips to Help Secure Your Identity:

- Medicare and Social Security will not call you to ask for your bank information or SSN.
- 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.

# What to Do if You Suspect You are a Victim of Identity Theft

## 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.

**Source:** *https://www.identitytheft.gov*

# Conclusion

One of the Senate Aging Committee's top priorities in the 116th Congress is to continue combating fraud that targets seniors. The Fraud Hotline has been instrumental in this fight, providing more than 1,500 people in 2018 with information on common scams and offering tips on how to avoid becoming victims of fraud. In addition, Fraud Hotline investigators have encouraged victims to report fraud to the appropriate law enforcement agencies to improve the government's data as well as its ability to prosecute the perpetrators of these scams. Committee investigators have even helped some victims recover thousands of dollars of their hard-earned retirement savings.

The Aging Committee has held hearings on seven of the top ten scams on this list. The Committee's hearings have helped raise public awareness to prevent seniors from falling victim to these scams, as well as to provide valuable oversight of the federal government's effort to combat these frauds and protect consumer. The Committee has pressed federal law enforcement agencies to combat fraud and put the criminals who prey on our nations' seniors behind bars.

While tangible progress has been made in countering a number of consumer scams, it is evident that more work remains to be done. In December 2018, the Federal Trade Commission reported that scammers are increasingly convincing older Americans to send cash to people pretending to be their grandchildren.

As the Aging Committee enters the 116th Congress, Chairman Collins and Ranking Member Casey intend to maintain the Committee's focus on frauds targeting seniors and will continue to work with their Senate colleagues to ensure that law enforcement has the tools it needs to pursue these criminals to encourage a more effective federal response to these scams.

This Fraud Book is designated to serve as a resource for seniors and others who wish to learn more about common scams and ways to avoid them. For further assistance, please contact the Aging Committee's Fraud Hotline at **1-855-303-9470** or visit our website at **www.aging.senate.gov**.

# Top Scams by State

These scams are based on calls into the Aging Committee's Fraud Hotline in 2018.

## Alabama
1. Elder Financial Abuse
2. IRS Impersonation Scam
3. Social Security Impersonation Scam
4. Romance Scam
5. Jamaican Lottery Scam

## Alaska
1. Unsolicited Phone Calls
2. Government Grant Scam

## Arizona
1. Computer Tech Support Scam
2. IRS Impersonation Scam
3. Unsolicited Phone Calls
4. Elder Financial Abuse
5. Social Security Impersonation Scam


## Arkansas
1. IRS Impersonation Scam
2. Sweepstakes Scam
3. Inheritance Scam
4. Health-Related Scam

## California
1. Elder Financial Abuse
2. Romance Scam
3. IRS Impersonation Scam
4. Computer Tech Support Scam
5. Sweepstakes Scam

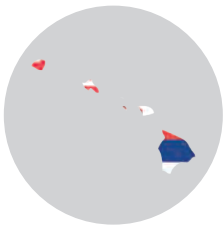
## Colorado
1. Elder Financial Abuse
2. IRS Impersonation Scam
3. Grandparent Scams
4. Romance Scam
5. Social Security Impersonation Scams

## Connecticut
1. Romance Scam
2. IRS Impersonation Scam
3. Identity Theft
4. Impending Law Suits Scams
5. Social Security Impersonation Scams

## Delaware
1. Charity Scams
2. Computer Tech Support Scam
3. Grandparent Scam
4. Identity Theft

## Florida
1. Unsolicited Phone Calls
2. Grandparent Scams
3. Computer Tech Support Scams
4. IRS Impersonation Scams
5. Elder Financial Abuse

## Georgia
1. Charity Scams
2. Elder Financial Abuse
3. Jamaican Lottery Scam
4. Timeshare Scams
5. Romance Scams



## Hawaii
1. Grandparent Scam
2. IRS Impersonation Scams
3. Romance Scams
4. Sweepstakes Scam

## Idaho
1. Social Security Impersonation Scam
2. Unclaimed Property Scam
3. IRS Impersonation Scams
4. Jamaican Lottery Scam
5. Unsolicited Phone Calls

## Illinois

1. Elder Financial Abuse
2. Sweepstakes Scam
3. Grandparent Scams
4. IRS Impersonation Scams
5. Unsolicited Phone Calls

## Indiana

1. Romance Scams
2. IRS Impersonation Scams
3. Identity Theft
4. Sweepstakes Scams
5. Mortgage Fraud

## Iowa

1. Jamaican Lottery Scam
2. Grandparent Scams
3. Impending Law Suit Scams
4. Romance Scams

## Kansas

1. Sweepstakes Scams
2. Elder Financial Abuse
3. Jamaican Lottery Scam
4. Unsolicited Phone Calls

## Kentucky

1. Grandparent Scams
2. Elder Financial Abuse
3. Romance Scams

## Louisiana

1. Consumer Complaints
2. IRS Impersonation Scams
3. Romance Scams

## Maine

1. IRS Impersonation Scam
2. Unsolicited Phone Calls
3. Computer Tech Support Scams
4. Social Security Impersonation Scam
5. Grandparent Scams

## Maryland

1. IRS Impersonation Scam
2. Grandparent Scams
3. Computer Tech Support Scams
4. Debt Collection Scams
5. Romance Scams

## Massachusetts

1. Unsolicited Phone Calls
2. Computer Tech Support Scams
3. Grandparent Scams
4. IRS Impersonation Scam
5. Impending Law Suit Scam

## Michigan

1. Computer Tech Support Scams
2. Romance Scams
3. IRS Impersonation Scams
4. Investment Fraud
5. Unsolicited Phone Calls

## Minnesota

1. IRS Impersonation Scam
2. Identity Theft
3. Impending Law Suit Scam
4. Sweepstakes Scams
5. Investment Fraud

## Mississippi

1. Sweepstakes Scam
2. Romance Scam

## Missouri

1. Computer Tech Support Scams
2. Elder Financial Abuse
3. Jamaican Lottery Scams
4. Identity Theft
5. Romance Scams

## Montana

1. Elder Financial Abuse
2. Unsolicited Phone Calls

# Top Scams by State (Cont.)

These scams are based on calls into the Aging Committee's Fraud Hotline in 2018.

**Nebraska**
1. IRS Impersonation Scam
2. Utility Scams
3. Elder Financial Abuse
4. Social Security Impersonation Scam
5. Unsolicited Phone Calls

**Nevada**
1. Computer Tech Support Scam
2. Elder Financial Abuse
3. Sweepstakes Scam

**New Hampshire**
1. Health-Related Scams

**New Jersey**
1. Consumer Complaints
2. Unsolicited Phone Calls
3. Computer Tech Support Scams
4. IRS Impersonation Scams
5. Social Security Impersonation Scams

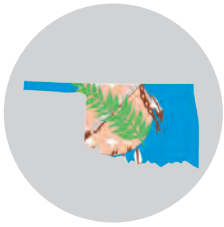
**New Mexico**
1. Impending Law Suit Scam
2. Romance Scams
3. Consumer Complaints
4. Identity Theft

**New York**
1. IRS Impersonation Scam
2. Unsolicited Phone Calls
3. Sweepstakes Scams
4. Elder Financial Abuse
5. Romance Scams

**North Carolina**
1. IRS Impersonation Scam
2. Elder Financial Abuse
3. Sweepstakes Scams
4. Romance Scams
5. Social Security Impersonation Scam

**North Dakota**
1. Inheritance Scams

**Ohio**
1. IRS Impersonation Scam
2. Unsolicited Phone Calls
3. Romance Scams
4. Elder Financial Abuse
5. Sweepstakes Scams



**Oklahoma**
1. Debt Collection Scams
2. Jamaican Lottery Scam
3. Romance Scams
4. Sweepstakes Scams

**Oregon**
1. Computer Tech Support Scams
2. Elder Financial Abuse
3. Grandparent Scams
4. IRS Impersonation Scams
5. Jamaican Lottery Scams

**Pennsylvania**
1. IRS Impersonation Scam
2. Unsolicited Phone Calls
3. Sweepstakes Scams
4. Computer Tech Support Scams
5. Elder Financial Abuse

# Top Scams by State (Cont.)

These scams are based on calls into the Aging Committee's Fraud Hotline in 2018.

## Rhode Island

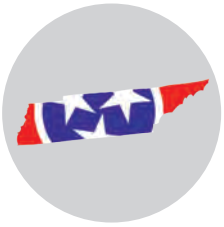
1. Elder Financial Abuse
2. IRS Impersonation Scam
3. Sweepstakes Scams
4. Unsolicited Phone Calls

## South Carolina

1. Consumer Complaints
2. Computer Tech Support Scam
3. IRS Impersonation Scams
4. Impending Law Suit Scams
5. Romance Scams

## South Dakota

1. Computer Tech Support Scams
2. Impending Law Suit Scams
3. Identity Theft
4. IRS Impersonation Scams



## Tennessee

1. Romance Scams
2. Computer Tech Support Scams
3. Grandparent Scams
4. Sweepstakes Scams
5. Unsolicited Phone Calls

## Texas

1. IRS Impersonation Scam
2. Sweepstakes Scams
3. Romance Scams
4. Elder Financial Abuse
5. Identity Theft

## Utah

1. IRS Impersonation Scam
2. Bank Fraud
3. Elder Financial Abuse
4. Romance Scams
5. Unsolicited Phone Calls

## Vermont

1. IRS Impersonation Scam

*Since the Fraud Hotline did not receive any calls from consumers in Vermont between 2017 and 2018, this list is based on call data from 2015 and 2016.

## Virginia

1. Sweepstakes Scams
2. Computer Tech Support Scams
3. Grandparent Scams
4. Identity Theft
5. IRS Impersonation Scam

## Washington

1. IRS Impersonation Scam
2. Grandparent Scams
3. Identity Theft
4. Inheritance Scams
5. Romance Scams

## West Virginia

1. Elder Financial Abuse
2. IRS Impersonation Scam

## Wisconsin

1. Can You Hear Me? Scam
2. Computer Tech Support Scams
3. Sweepstakes Scams
4. Health-Related Scams
5. Grandparent Scams

## Wyoming

1. Romance Scams

# **Appendix 1:** 2018 Complete Aging Fraud Hotline Statistics

| Scam Type | Total |
|---|---|
| IRS Scam | 282 |
| Unsolicited Phone Calls | 149 |
| Sweepstakes/Jamaican Lottery Scam | 99 |
| Computer Scam | 82 |
| Elder Abuse | 78 |
| Grandparent Scam | 71 |
| Romance Scam | 68 |
| Social Security Fraud | 64 |
| Impending Law Suits | 54 |
| Identity Theft | 45 |
| Consumer Related | 43 |
| Charity Scam | 30 |
| Debt Collection Scam | 25 |
| Health-Related Scam | 19 |
| Investment Fraud | 17 |
| Bank Fraud | 15 |
| Government Grant | 15 |
| Utility Scam | 15 |
| Can You Hear Me? Scam | 13 |
| Check Scam | 12 |
| Legal Referral | 12 |
| Mortgage Fraud | 12 |
| Mail Scam | 10 |
| Timeshare Scam | 8 |
| Inheritance Scam | 7 |
| Phishing Scam | 5 |
| Unclaimed Property Scam | 5 |
| Pension/Retirement Savings Fraud | 3 |
| Spam Email | 3 |
| Wire Fraud | 3 |
| IRS Fraudulent Tax Returns | 2 |
| Kidnapping Scam | 2 |
| Grand Jury Impersonation Scam | 2 |
| Long-Term Care | 1 |
| Robbery/Theft | 1 |
| Miscellaneous** | 260 |
| **TOTAL** | **1509** |

| State | Total |
|---|---|
| Alabama | 8 |
| Alaska | 3 |
| Arizona | 26 |
| Arkansas | 5 |
| California | 91 |
| Colorado | 19 |
| Connecticut | 11 |
| Delaware | 5 |
| Florida | 105 |
| Georgia | 9 |
| Hawaii | 5 |
| Idaho | 8 |
| Illinois | 19 |
| Indiana | 6 |
| Iowa | 6 |
| Kansas | 8 |
| Kentucky | 6 |
| Louisiana | 6 |
| Maine | 489 |
| Maryland | 79 |
| Massachusetts | 18 |
| Michigan | 30 |
| Minnesota | 8 |
| Mississippi | 4 |
| Missouri | 17 |

| State | Total |
|---|---|
| Montana | 2 |
| Nebraska | 7 |
| Nevada | 3 |
| New Hampshire | 1 |
| New Jersey | 28 |
| New Mexico | 7 |
| New York | 82 |
| North Carolina | 22 |
| North Dakota | 1 |
| Ohio | 18 |
| Oklahoma | 6 |
| Oregon | 14 |
| Pennsylvania | 160 |
| Rhode Island | 5 |
| South Carolina | 16 |
| South Dakota | 7 |
| Tennessee | 15 |
| Texas | 87 |
| Utah | 9 |
| Virginia | 15 |
| Washington | 11 |
| West Virginia | 3 |
| Wisconsin | 9 |
| Wyoming | 1 |
| Unknown | 17 |

# **Appendix 2.** Fraud Resources

## General Consumer Complaints

| Agency | Website | Phone Number |
|---|---|---|
| Better Business Bureau | www.bbb.org | Use zip code to find local caller's local BBB |
| National Do-Not-Call Registry | www.donotcall.org | 1-888-382-1222 |
| National Do-Not-Call Complaint Form | www.fcc.gov/complaints | 1-888-225-5322 |
| USA.gov for Seniors | http://www.usa.gov/Topics/Seniors.shtml | 1-800-333-4636 |
| AARP Fraud Fighter Call Center | http://www.aarp.org/content/dam/aarp/money/scams_fraud/2013-10/Who-To-Contact-AARP.PDF | 1-877-908-3360 |
| AARP Fraud Watch Network | www.aarp.org/fraudwatchnetwork | 1-800-646-2283 |
| Local/State AG Office | http://www.naag.org/current-attorneys-general.php | |
| US Senator/Rep. Office for Constituent Casework | http://www.senate.gov/general/contact_information/senators_cfm.cfm<br>http://www.house.gov/ | |
| Federal Trade Commission Sentinel Network | http://www.ftc.gov/enforcement/consumer-sentinel-network | 1-877-701-9595 |
| Federal Trade Commission Consumer Response Center | http://www.consumer.ftc.gov/ | 1-877-382-4357 |
| Federal Communications Commission | http://www.fcc.gov/ | 1-888-225-5322 |
| State/Local Consumer Protection Agencies | http://www.usa.gov/directory/stateconsumer/index.shtml | |
| Assist Guide Information Services – Government Agency/Programs by State | http://www.agis.com/listing/default.aspx | |
| DOJ Elder Justice Initiative | www.justice.gov/elderjustice/ | 1-202-514-2000 (DOJ Main Switchboard) |
| Area Agency on Aging | http://www.n4a.org/ | |
| IRS Scam Reporting Hotline | https://www.treasury.gov/tigta/contact_report_scam.shtml | 1-800-366-4484 |
| HHS OIG | http://www.hhs.gov/grants/grants/avoid-grant-scams/index.html | 1-800-447-8477 |
| National Center for Victims of Crime | https://www.victimsofcrime.org/ | 1-855-484-2846 |
| FINRA Securities Helpline for Seniors | http://www.finra.org/investors/finra-securities-helpline-seniors | 1- 844-574-3577 |
| Center for Elder Rights Advocacy | http://www.legalhotlines.org/legal-assistance-resources.html | |

## Resources – Issue Area

### Computer Fraud

*If receiving spam email, forward the spam email to spam@uce.gov . This website is managed by the Federal Trade Commission.*

| Agency | Website | Phone Number |
|---|---|---|
| Internet Crime Complaint Center (IC3) | www.ic3.gov/crimeschemes.aspx | |
| Federal Trade Commission | http://www.consumer.ftc.gov/articles/0346-tech-support-scams | 1-877-382-4357 |

### Elder Abuse

| Agency | Website | Phone Number |
|---|---|---|
| Local/State AG Office | http://www.naag.org/current-attorneys-general.php | |
| National Adult Protection Services Association | Find local APS Association: www.napsa-now.org/get-help/help-in-your-area/ | |
| DOJ Elder Justice Initiative | www.justice.gov/elderjustice/ | 1-202-514-2000 (DOJ Main Switchboard) |
| Financial exploitation | www.eldercare.gov | 1-800-677-1116 |
| Center for Elder Rights Advocacy | http://www.legalhotlines.org/legal-assistance-resources.html | |

### Health-Related Scams

| Agency | Website | Phone Number |
|---|---|---|
| Federal Communications Commission | www.fcc.gov/complaints | 1-888-225-5322 |
| Federal Trade Commission | http://www.consumer.ftc.gov/blog/robocall-scams-push-medical-alert-systems | 1-888-382-1222 |
| Medicare.gov | State/Local resources: www.medicare.gov/contacts/topic-search-criteria.aspx | |
| DHHS IG to report Medicare Fraud | https://forms.oig.hhs.gov/hotlineoperations/ | 1-800-447-8477 |
| Medicare Ombudsman's Office | http://www.medicare.gov/claims-and-appeals/medicare-rights/get-help/ombudsman.html | |
| Medicare Rights Center | http://www.medicarerights.org/ | 1-800-333-4114 |
| Health Insurance Marketplace Fraud | DHHS IG Marketplace Consumer Fraud Hotline: https://oig.hhs.gov/fraud/consumer-alerts/alerts/marketplace.asp | 1-800-318-2596 |

## Identity Theft

*Call one of the three national credit bureaus to place a scam 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)

| Agency | Website | Phone Number |
|---|---|---|
| Local Police Department | | Check with your local police department. Many departments have non-emergency numbers you may call to file a report. |
| FTC ID Theft Hotline | https://www.identitytheft.gov/ | 1-877-438-4338 |
| FTC Identity Theft Resource Center | http://www.consumer.ftc.gov/features/feature-0014-identity-theft | 1-888-400-5530 |
| IRS Identity Protection Specialized Unit | http://www.irs.gov/Individuals/Identity-Protection | 877-777-4778 |
| Office of the Comptroller of the Currency | http://www.occ.gov/topics/bank-operations/financial-crime/identity-theft/index-identity-theft.html | 1-202-649-6800 |
| SSA – File a report of theft or fraudulent use of SS number | http://www.ssa.gov/pubs/EN-05-10064.pdf | 1-800-269-0271 |

## Investment/Securities Fraud

| Agency | Website | Phone Number |
|---|---|---|
| FINRA Securities Helpline for Seniors | http://www.finra.org/investors/finra-securities-helpline-seniors | 1- 844-574-3577 |
| Consumer Financial Protection Bureau (CFPB) | http://www.consumerfinance.gov | 1-855-411-2372 |
| CFPB ombudsman – consumer who has a process issue from using CFPB complaint function | http://www.consumerfinance.gov/ombudsman/ | 1-855-830-7880 |
| Financial Industry Regulatory Authority (FINRA) | www.finra.org | 1-800-289-9999 |
| Better Business Bureau | www.bbb.org | |
| Securities Investor Protection Corporation (SIPC) | http://www.sipc.org/ | 1-202-371-8300 |
| Federal Reserve Consumer Help | http://www.federalreserveconsumerhelp.gov/ | 1-888-851-1920 |

## Jamaican Lottery Scam

| Agency | Website | Phone Number |
|---|---|---|
| AARP Fraud Fighter Call Center | http://www.aarp.org/content/dam/aarp/money/scams_fraud/2013-10/Who-To-Contact-AARP.PDF | 1-800-646-2283 |
| Department of Homeland Security Tip Line | https://www.ice.gov/tipline | 1-866-347-2423 |
| Postal Inspector | https://postalinspectors.uspis.gov/ | 1-877-876-2455 |
| Western Union Fraud Unit | https://www.westernunion.com/us/en/fraudawareness/fraud-report-to-authorities.html | 1-800-448-1492 |
| Moneygram Fraud Unit | http://corporate.moneygram.com/compliance/fraud-prevention | 1-800-666-3947 |
| GreenDot MoneyPak Report Fraud | https://www.moneypak.com/protectyourmoney.aspx | |
| FBI Field Office | http://www.fbi.gov/contact-us/field | |
| Secret Service Field Office | http://www.secretservice.gov/field_offices.shtml | |

## PCH/Sweepstakes Fraud

| Agency | Website | Phone Number |
|---|---|---|
| Postal Inspector | https://postalinspectors.uspis.gov/ | 1-877-876-2455 |
| AARP Fraud Fighter Call Center | http://www.aarp.org/content/dam/aarp/money/scams_fraud/2013-10/Who-To-Contact-AARP.PDF | 1-800-646-2283 |
| FCC | www.fcc.gov/complaints | 1-888-225-5322 |
| FTC Consumer Response Center | http://www.consumer.ftc.gov/ | 1-877-382-4357 |
| PCH Fraud Department | | 1-800-392-4190 |
| PCH Email Scams | Forward to abuse@pch.com | |

## Mortgage Fraud

| Agency | Website | Phone Number |
|---|---|---|
| Consumer Financial Protection Bureau (CFPB) | http://www.consumerfinance.gov/ | 1-855-411-2372 |
| Foreclosure Prevention Counseling – HUD's Housing Counseling Program | www.hud.gov/offices/hsf/sfh/hcc/fc/ | Find State counseling program |
| HUD OIG Fraud Hotline | https://www.hudoig.gov/report-fraud | 1-800-347-3735 |

## Payday Lending

| Agency | Website | Phone Number |
|---|---|---|
| Consumer Financial Protection Bureau (CFPB) | http://www.consumerfinance.gov/ | 1-855-411-2372 |
| FTC Consumer Response Center | http://www.consumer.ftc.gov/ | 1-877-382-4357 |

## Social Security Fraud

*Contact local Social Security field office to place a freeze on any changes to their Social Security account to prevent future misuse of their Social Security benefits.*

Call one of the three national credit bureaus to place a scam 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)

| Agency | Website | Phone Number |
|---|---|---|
| SSA OIG | https://www.socialsecurity.gov/fraudreport/oig/public_fraud_reporting/form.htm | 1-800-269-0271 |
| Financial Exploitation | www.eldercare.gov | 1-800-677-1116 |
| Information on Representative Payee for victim's social security benefits | http://www.socialsecurity.gov/payee/faqrep.htm#a0=2. | |
| SSA | https://secure.ssa.gov/ICON/main.jsp | 1-800-772-1213 |

## Timeshare Scam

| Agency | Website | Phone Number |
|---|---|---|
| State Attorney General | http://www.naag.org/current-attorneys-general.php | |
| FTC Consumer Response Center | http://www.consumer.ftc.gov/ | 1-877-382-4357 |
| Better Business Bureau | www.bbb.org | |
| Internet Crime Complaint Center (IC3) | www.ic3.gov/crimeschemes.aspx | |

## Grandparent Scam

| Agency | Website | Phone Number |
|---|---|---|
| FTC Consumer Response Center | http://www.consumer.ftc.gov/ | 1-877-382-4357 |
| State Attorney General | http://www.naag.org/current-attorneys-general.php | |
| Department of Homeland Security Tip Line | https://www.ice.gov/tipline | 1-866-347-2423 |
| FBI Field Office | http://www.fbi.gov/contact-us/field | |
| Secret Service Field Office | http://www.secretservice.gov/field_offices.shtml | |

# State Attorneys General

**Alabama**
(334) 242-7300

**Alaska**
(907) 269-5100

**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

**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) 373-1110

**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

**Ohio**
(614) 466-4986

**Oklahoma**
(405) 521-3921

**Oregon**
(503) 378-4400

**Pennsylvania**
(717) 787-3391

**Rhode Island**
(401) 274-4400

**South Carolina**
(803) 734-3970

**South Dakota**
(605) 773-3215

**Tennessee**
(615) 741-3491

**Texas**
(512) 463-2100

**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

**Puerto Rico**
(787) 721-2900

**US Virgin Islands**
(340) 774-5666

# **Appendix 3.** Cut out Scam Prevention Tip Cards

Please cut out these cards and place them by your phone. Give one to a friend, family member, or neighbor. We hope these cards may be a useful tool to help protect you against the deceptive means scammers use to try to get your money and personal information.

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


UNITED STATES
E PLURIBUS UNUM
SENATE


UNITED STATES
E PLURIBUS UNUM
SENATE

# References

1 U.S. Congress, Senate Committee on Finance, *Tax Schemes and Scams During the 2015 filing Season*, hearings, 114th Congress, 1st sess., March 12, 2015 (Washington, DC: GPO, 2015).

2 TIGTA, *Semiannual Report to Congress: April 1, 2018 – September 30*, 2018; Pg. 35 (accessed on December 10, 2018), at https://www.treasury.gov/tigta/semiannual/semiannual_sept2018.pdf.

3 TIGTA, *Semiannual Report to Congress: April 1, 2018 – September 30, 2018*; Pg. 35 (accessed on December 10, 2018), at https://www.treasury.gov/tigta/semiannual/semiannual_sept2018.pdf.

4 TIGTA Conference Call with Aging Committee, January 18, 2017.

5 U.S. Congress, Senate Special Committee on Aging, *Catch Me If You Can: The IRS Impersonation Scam and the Government's Response*, hearings, 114th Congress, 1st sess., April 15, 2015 (Washington, DC: GPO, 2015).

6 Internal Revenue Service, *Tax Scams/Consumer Alerts*, (accessed January 22, 2017), at https://www.irs.gov/newsroom/tax-scams-consumer-alerts.

7 TIGTA Conference Call with Aging Committee, January 7, 2016.

8 Internal Revenue Service, "IRS Warns Taxpayers to Guard Against New Tricks by Scam Artists; Losses Top $20 Million," August 6, 2015 (accessed January 22, 2017), at https://www.irs.gov/newsroom/irs-warns-taxpayers-to-guard-against-new-tricks-by-scam-artists-losses-top-20-million

9 Internal Revenue Service, "Five Easy Ways to Spot a Scam Phone Call," August 6, 2015, (accessed January 22, 2017), https://www.irs.gov/newsroom/five-easy-ways-to-spot-a-scam-phone-call.

10 Treasury Inspector General for Tax Administration, "IRS Impersonation Scam Update," April 21, 2016 (accessed January 22, 2017), https://www.treasury.gov/tigta/irs_scam_updates.shtml.

11 TIGTA, *Semiannual Report to Congress: April 1, 2018 – September 30*, 2018; Pg. 35 (accessed on December 10, 2018), at https://www.treasury.gov/tigta/semiannual/semiannual_sept2018.pdf.

12 Ibid.

13 Associated Press, "Man gets 14 years in prison for scam that took millions with fake IRS calls," July 8, 2015.

14 TIGTA, Email to Aging Committee, February 13, 2018.

15 Ibid.

16 Ibid.

17 Ibid.

18 Ibid.

19 Department of Justice, "Dozens of Individuals Indicted in Multimillion-Dollar Indian Call Center Scam Targeting U.S. Victims," October 27, 2016, at https://www.justice.gov/opa/pr/dozens-individuals-indicted-multimillion-dollar-indian-call-center-scam-targeting-us-victims.

20 TIGTA Conference Call with Aging Committee, December 9, 2016.

21 Ibid.

22 Testimony of BBB Institute for Marketplace Trust President Genie Barton, in U.S. Congress, Senate Special Committee on Aging, *Still Ringing off the Hook: An Update on Efforts to Combat Robocalls*, hearings, 115th Cong., 1st sess., October 4, 2017.

23 TIGTA, *Semiannual Report to Congress: April 1, 2018 – September 30, 2018*; Pg. 35 (accessed on December 10, 2018), at https://www.treasury.gov/tigta/semiannual/semiannual_sept2018.pdf.

24 Internal Revenue Service, *Private Debt Collection*, August 7, 2017 (accessed February 2, 2018) at [page no longer available].

25 Ibid.

26 TIGTA email to Senate Aging Committee on February 5, 2018.

27 "To ratify the authority of the Federal Trade Commission to establish a do-not-call registry." Public Law 108-82. 108th Congress, 1st sess.

28 FCC; Notice of Inquiry, FCC 17-89, July 14, 2017 (accessed September 26, 2017), apps.fcc.gov/edcos_public/attachmatch/FCC-17-89A1.pdf

29 Federal Trade Commission. Do Not Call Data Book 2018. December 6, 2018. https://www.ftc.gov/system/files/documents/reports/national-do-not-call-registry-data-book-fiscal-year-2018/2018_dnc_data_book_0.pdf pg. 6 Accessed on January 1, 2019.

30 U.S. Congress, Senate Special Committee on Aging, *Ringing Off the Hook: Examining the Proliferation of Unwanted Calls*, hearings, 114th Cong., 1st sess., June 10, 2015.

31 Ibid.

32 FCC, *Fact Sheet on Consumer Protection Proposal*, June 18, 2015 (accessed September 24, 2017), https://www.fcc.gov/document/fact-sheet-consumer-protection-proposal.

33 *Robocall Strike Force Report*, October 26, 2016 (accessed on September 27, 2017), p. 1, https://transition.

fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf

34 Rupy, Kevin, "USTelecom Calls for Flexibility in Blocking Robocalls," July 10, 2017 (accessed September 28, 2017), https://www.ustelecom.org/blog/ustelecom-calls-flexibility-blocking-robocalls.

35 U.S. Senate Special Committee on Aging, "Aging Committee Leaders Collins and Casey Urge FCC to Support Proposed Rule to Limit Robocalls," press release, March 23, 2017 (accessed on February 5, 2018), at https://www.aging.senate.gov/press-releases/aging-committee-leaders-collins-and-casey-urge-fcc-to-support-proposed-rule-to-limit-robocalls.

36 Federal Communications Commission, "FCC Adopts Rules to Help Block Illegal Robocalls," November 16, 2017 (accessed February 8, 2018), [link missing].

37 Federal Trade Commission, "FTC Challenges Innovators to do Battle with Robocallers," press release, October 18, 2012 (accessed February 8, 2018), at https://www.ftc.gov/news-events/press-releases/2012/10/ftc-challenges-innovators-do-battle-robocallers

38 Federal Trade Commission, "FTC Announces Robocall Challenge Winners," press release, April 2, 2013 (accessed January 22, 2017), www.ftc.gov/news-events/press-releases/2013/04/ftc-announces-robocall-challenge-winners.

39 Ibid.

40 Federal Trade Commission, "FTC Announces New Robocall Contests to Combat Illegal Automated Calls," March 4, 2015 (accessed January 22, 2017), www.ftc.gov/news-events/press-releases/2015/

41 Ibid.

42 Federal Trade Commission, "FTC Awards $25,000 Top Cash Prize for Contest-Winning Mobile App that Blocks Illegal Robocalls," www.ftc.gov/news-events/press-releases/2015/08/ftc-awards-2500-top-cash-prize-contest-winning-mobile-app-blocks.

43 Ibid.

44 Federal Trade Commission; "Consumer Information: Prize Scams" (accessed January 18, 2017), at https://www.consumer.ftc.gov/articles/0199-prize-scams.

45 Federal Trade Commission; "Consumer Sentinel Network Data Book for January-December 2015," February 2016 (accessed January 22, 2017), p. 80, at https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2015/160229csn-2015databook.pdf.

46 Federal Trade Commission; "Consumer Sentinel Network Data Book for January-December 2017," February 2018 (accessed December 11, 2018), p. 6, at https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2017/consumer_sentinel_data_book_2017.pdf.

47 Moyer, Marriell, "Lebanon County Elderly Being Victimized by Phone Scam," *Lebanon Daily News*, July 13, 2017, at https://www.ldnews.com/story/news/local/2017/07/13/lebanon-county-elderly-being-victimized-phone-scams/471992001.

48 U.S. Congress, Senate Special Committee on Aging, *876-SCAM: Jamaican Phone Fraud Targeting Seniors*, hearings, 113th Congress, 1st sess., March 13, 2013 (Washington, DC: GPO, 2013).

49 FairPoint Communications, "FairPoint applauds Western Union decision to shut down services in Jamaican hotbed of phone scamming operations," *BEWARE: Scams from Area Code 876* (accessed January 22, 2017), [link unavailable].

50 U.S. Congress, *876-SCAM*, S. 6-7.

51 U.S. Department of Homeland Security, U.S. Immigration and Customs Enforcement, "Jamaican man first to be extradited to face fraud charges in lottery scam," press release, February 12, 2015 (accessed January 22, 2017), https://www.ice.gov/news/releases/jamaican-man-first-be-extradited-face-fraud-charges-lottery-scam.

52 Federal Bureau of Investigation, "Jamaican Man Sentenced to Prison for Involvement in International Lottery Fraud Scheme," November 25, 2015 (accessed January 22, 2017), https://www.fbi.gov/contact-us/field-offices/minneapolis/news/press-releases/jamaican-man-sentenced-to-prison-for-involvement-in-international-lottery-fraud-scheme.

53 Tillerson, Rex W., "Remarks: Press Availability with Jamaican Prime Minister Andrew Holness," February 7, 2018 (accessed February 10, 2018), https://www.state.gov/secretary/remarks/2018/02278085.htm.

54 Ibid.

55 U.S. Congress, Senate Special Committee on Aging, *Virtual Victims: When computer Tech Support Becomes a Scam*, hearings, 114th cong., 1st sess., October 21, 2015, 114-22, (Washington, DC: GPO, 2015).

56 Ibid.

57 Federal Trade Commission, Staff Briefing, Dirksen Senate Office Building, G16, Washington, DC, October 14, 2015.

58 Internet Crime Complaint Center; "2017 Internet Crime Report," 2018 (accessed on December 19 2018), pp. 14 https://pdf.ic3.gov/2017_IC3Report.pdf.

59 Ibid.

60 U.S. Congress, Senate Special Committee on Aging, *Virtual Victims: When computer Tech Support Becomes a Scam*, hearings, 114th cong., 1st sess., October 21, 2015, 114-22, (Washington, DC: GPO, 2015).

61 U.S. Congress, Senate Special Committee on Aging, *Virtual Victims: When computer Tech Support*

*Becomes a Scam*, hearings, 114th cong., 1st sess., October 21, 2015, 114-22, (Washington, DC: GPO, 2015).

62 Complaint at 19 *FTC v. PCCare 247, Inc., et. al.*, No. 12-cv-7189, S.D.N.Y, ECF No. 8.

63 Federal Trade Commission, "FTC Testifies on Efforts to Stop Illegal Tech Support Scams Before Senate Special Committee on Aging, October 21, 2015 (accessed January 22, 2017), https://www.ftc.gov/news-events/press-releases/2015/10/ftc-testifies-efforts-stop-illegal-tech-support-scams-senate.

64 Department of Justice, "Seven Charged in International 'Tech Support Scam,'" press release, May 12, 2017 (accessed on February 20, 2018), https://www.justice.gov/usao-sdil/pr/seven-charged-international-tech-support-scam.

65 Ibid.

66 Ibid.

67 Ibid.

68 Attorney General's Annual Report to Congress on Department of Justice Activities to Combat Elder Abuse and Financial Exploitation. October 18, 2018. Pg. 16. (accessed on December 15, 2018).

69 Ibid.

70 Ibid.

71 Elton, Catherine, "The Fleecing of America's Elderly," *Consumers Digest*, November 10, 2012.

72 GAO, *Elder Justice: Stronger Federal Leadership Could Enhance National Response to Elder Abuse*, March 21, 2011, p. 9.

73 Ibid., 14.

74 Ibid., 15.

75 U.S. Department of Justice, "Financial Exploitation FAQs," *Elder Justice Initiative*, accessed January 18, 2016, https://www.justice.gov/file/1064511/download.

76 MetLife Market Institute, The National Committee for the Prevention of Elder Abuse, and the Center for Gerontology at Virginia Polytechnic Institute and State University, *Elder Financial Abuse: Crimes of Occasion, Desperation, and Predation Against America's Elders*, June 2011, p. 8.

77 Ibid.

78 Ibid., 10.

79 Culley, Denis and Martin, Jaye, *No Higher Calling – Representing Victims of Fianacial Exploitation*, Bifocal 34, no. 5 (May-June), p. 89.

80 Department of Justice, "Deputy Attorney General James M. Cole Speaks at the White House World Elder Abuse Awareness Day Event," speeches, accessed January 19, 2016, at https://www.justice.gov/file/1064511/download.

81 U.S. Government Accountability Office, *Elder Justice: National Strategy needed to Effectively Combat Elder Exploitation*, GAO-13-110, November, 2012, at https://www.gao.gov/assets/660/650074.pdf.

82 GAO, *Elder Justice*, 22.

83 Ibid., 25-26.

84 Elder Abuse Prevention and Prosecution Act, Public Law no. 115-70, October 18, 2017.

85 U.S. Congress, Congressional Record, 114th Cong., 1st sess., 2015, S7595-S7596.

86 Metcalf, Andrew, "Caretaker Sentenced for Stealing More than $400,000 from 87-year-old Bethesda Man," *Bethesda Magazine*, October 10, 2015.

87 Ibid.

88 Betts, Stephen, "Belfast Lawyer Gets 30 Months in Prison for Bilking Elderly clients," *Bangor Daily News*, March 4, 2016 (accessed on January 22, 2017), at http://bangordailynews.com/2016/03/04/news/midcoast/belfast-lawyer-gets-30-months-in-prison-for-bilking-elderly-clients.

89 Ibid.

90 Ibid.

91 Ibid.

92 Russell, Eric, "Victim of a Long Con Lives Out her Days Penniless in a Fryeburg Nursing Home," *Maine Sunday Telegram*, November 27, 2016 (accessed January 22, 2017), https://www.pressherald.com/2016/11/27/victim-of-a-long-con-lives-out-her-days-penniless-in-a-fryeburg-nursing-home.

93 Ibid.

94 Ibid.

95 U.S. Government Accountability Office, *Elder Abuse: The Extent of Abuse by Guardians is Unknown, but Some Measures Exist to Help Protect Older Adults*, GAO-17-33, November 2016, https://www.gao.gov/assets/690/681088.pdf.

96 Moyer, Marriell, "Lebanon County Elderly Being Victimized by Phone Scam," *Lebanon Daily News*, July 13, 2017, at https://www.ldnews.com/story/news/local/2017/07/13/lebanon-county-elderly-being-victimized-phone-scams/471992001.

97 Federal Trade Commission; "Consumer Sentinel Network Data Book for January-December 2015," February 2016 (accessed January 22, 2017), p. 82, at https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2015/160229csn-2015databook.pdf.

98 Federal Trade Commission; "Consumer Sentinel Network Data Book for January-December 2017," February 2018 (accessed December 12, 2018), p. 93, at https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2017/consumer_sentinel_data_book_2017.pdf.

99 Testimony of Lois Greisman, in U.S. Congress, Senate Special Committee on Aging, *Hanging Up on Phone Scams: Progress and Potential Solutions to this Scourge*, hearings, 113th Cong., 2nd sess., July 16, 2014, S.Hrg. 113-20 (Washington, DC: GPO, 2014).
100 Attorney General's Annual Report to Congress on Department of Justice Activities to Combat Elder Abuse and Financial Exploitation. October 18, 2018. Pg. 16-17. (accessed on December 15, 2018).
101 Ibid.
102 Ibid.
103 Ibid.
104 Smith, Aaron and Anderson, Monica, "5 Facts About Online Dating," *Pew Research Center*, February 29, 2016 (accessed on February 16, 2018), at http://www.pewresearch.org/fact-tank/2016/02/29/5-facts-about-online-dating.
105 Ibid.
106 FBI, *2016 Computer Crime Report*, accessed February 14, 2018, p. 17, at http://www.pdf.ic3.gov/2016_IC3Report.pdf.
107 Federal Trade Commission; "Consumer Information, Online Dating Scams," accessed January 22, 2017, at https://www.consumer.ftc.gov/articles/0004-online-datingscams.
108 Federal Bureau of Investigation, "Looking for Love? Beware of Online Dating Scams," press release, February 14, 2013 (accessed January 22, 2017), https://archives.fbi.gov/archives/sandiego/press-releases/2013/looking-for-love-beware-of-online-dating-scams.
109 FBI, *2017 Internet Crime Report*, accessed December 17, 2018, pp. 22-23, https://pdf.ic3.gov/2017_IC3Report.pdf.
110 FBI, *2014 Computer Crime Report*, accessed January 22, 2017, p. 42, https://pdf.ic3.gov/2014_IC3Report.pdf.
111 Ibid.
112 U.S. Army Criminal Investigation Command Public Affairs, "Army investigators warn public about romance scams," U.S. Army, July 30, 2014 (accessed January 22, 2017), at https://www.army.mil/article/130861/Army_investigators_warn_public_about_romance_scams.
113 Halpern, Mollie, "Podcast and Radio: Romance Scams," *FBI This Week*, February 5, 2015 (accessed January 22, 2017), https://www.fbi.gov/audio-repository/news-podcasts-thisweek-romance-scams.mp3/view.
114 National Center on Elder Abuse, "Elder Abuse and its Impact: What You Must Know," accessed Januaty 19, 2016, [link dead].
115 Borland, Jim. Is that Phone Call from US? Social Security Administration. October 30, 2017. https://blog.ssa.gov/is-that-phone-call-from-us/ (accessed on December 12, 2018).
116 https://www.ssa.gov/phila/scams.htm
117 Federal Trade Commission, "Consumer Sentinel Network Data Book for January-December 2017," February 2018 (accessed December 17, 2018), p. 6, at https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2017/consumer_sentinel_data_book_2017.pdf.
118 Federal Trade Commission, "Consumer Sentinel Network Data Book for January-December 2017," February 2018 (accessed December 17, 2018), p. 16, at https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2017/consumer_sentinel_data_book_2017.pdf.
119 Marte, Jonnelle, "You can now request copies of the phony tax returns filed in your name," *Washington Post*, November 10, 2015.
120 IRS, "Key IRS Identity Theft Indicators Continue Dramatic Decline in 2017; Security Summit Marks 2017 Progress Against Identity Theft," press release, February 8, 2018 (accessed on February 10, 2018), https://www.irs.gov/newsroom/key-irs-identity-theft-indicators-continue-dramatic-decline-in-2017-security-summit-marks-2017-progress-against-identity-theft.
121 Ibid.
122 *Medicare Access and CHIP Reauthorization Act of 2015*, Public Law 114-10, 114th Congress, 2nd sess.
123 Centers for Medicare and Medicaid; "Your Medicare Card," accessed February 8, 2018, at https://www.medicare.gov/forms-help-resources/your-medicare-card.
124 U.S. Congress, Senate Special Committee on Aging, *Protecting Seniors from Identity Theft: Is the Federal Government Doing Enough?*, hearings, 114th Cong., 1st sess., October 7, 2015.
125 Ibid.
126 Hacket, Robert, "Equifax Underestimated by 2.5 Million the Number of Potential Breach of Victims," *Fortune*, October 2, 2017 (accessed on February 26, 2018), http://fortune.com/2017/10/02/equifax-credit-breach-total.
127 Better Business Bureau, "Scam Alert: Con Artist Bank on Equifax Breach," *Better Business Bureau for Marketplace Trust*, September 22, 2017 (accessed on September 27, 2017), https://www.bbb.org/council/news-events/bbb-scam-alerts/2017/09/scam-alert-con-artists-bank-on-equifax-breach.
128 Better Business Bureau; Scam Tracker, https://www.bbb.org/scamtracker/us.

# 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**