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

Note: This document has been printed for information purposes. It does not represent either findings or recommendations formally adopted by the Committee.

Table of Contents

Dear Friends 3

Executive Summary 5

2017 Key Figures 7

Abbreviations 8

Top Ten Types of Scams Reported to the Hotline

- IRS Impersonation Scams 9
- Robocalls and Unsolicited Phone Calls 14
- Sweepstakes Scams / Jamaican Lottery Scam 18
- "Can You Hear Me?" Scams 20
- Grandparent Scams 22
- Computer Tech Support Scam 24
- Romance Scams 27
- Elder Financial Abuse 29
- Identity Theft 32
- Government Grant Scams 35

Conclusion 36

Top Scams By State 37

Appendix

- Appendix 1: 2017 Complete Aging Fraud Hotline Statistics 41
- Appendix 2: Aging Committee's Top 10 Historical Data 42
- Appendix 3: Fraud Resource 43
- Appendix 4: Cut out Scam Prevention Tip Cards 49

References 50

Dear Friends:

Our nation's seniors worked hard their entire lives and saved for retirement. Unfortunately, many criminals target them and seek to rob them of their hard-earned savings. Far too many older Americans are being financially exploited by strangers over the telephone, through the mail, and, increasingly, online. Worse yet, these seniors may also be targeted by family members or by other people they trust. Many of these crimes are not reported because the victims are afraid that the perpetrator may retaliate, are embarrassed that they have been scammed, or sometimes simply because they are unsure about which law enforcement or consumer protection agency they should contact. Additionally, some seniors do not realize they have been the victims of fraud.

The U.S. Senate Special Committee on Aging has made consumer protection and fraud prevention a major focus of its work. In recent years, the Committee has held hearings examining telephone scams, tax-related schemes, Social Security fraud, and the implications of payday loans and pension advances for seniors, among other issues. 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.

The Senate Aging Committee remains committed to protecting older Americans against fraud and to bringing greater awareness of this pervasive problem. The Fraud Hotline has been successful in meeting both of those goals, assisting individuals who contacted the Committee over the telephone or through the online form on the Committee's website. The Fraud Hotline allows the Committee to maintain a detailed record of common fraud schemes targeting seniors. This record informs the efforts of the Committee and, ultimately, the work of the United States Congress.

Additionally, the Fraud Hotline offers real help to victims and to those targeted by scammers. Committee staff and investigators who have experience dealing with a variety of scams and fraud speak directly with callers and can assist callers by providing them with important information regarding steps they can take, including where to report the fraud and ways to reduce the likelihood that the senior will become a victim or a repeat victim.

Investigators typically refer seniors to the relevant local, state, and/or federal law enforcement entities with jurisdiction over the particular scam. In addition to law enforcement, Fraud Hotline investigators may also direct seniors to other resources, such as consumer protection groups, legal aid clinics, congressional caseworkers, or local nonprofits that assist seniors.

Over the past year, more than 1,400 individuals all across the country contacted the Fraud Hotline. Since the Fraud Hotline's inception in 2013, more than 6,800 individuals from all 50 states have contacted the Committee's Fraud Hotline to report a possible scam. Consumer advocacy organizations, community centers, and local law enforcement have provided invaluable assistance to the Committee by encouraging consumers to call the Fraud Hotline to document scams. We would like to thank all of the groups and governmental entities that work with us to fight fraud.

In an effort to educate seniors on emerging trends and to help protect them from becoming victims, this Fraud Book features the top ten scams reported to our Hotline last year. In addition, it includes resources for consumers who wish to report scams to state and federal agencies.

The range and frequency of scams perpetrated against seniors that were reported to the Fraud Hotline in 2017 demonstrate the extent of this epidemic. In 2018, the Aging Committee intends to build on its successful efforts to investigate and stop scams aimed at our nation's seniors and ensure that federal agencies are aggressively pursuing the criminals who commit these frauds.

Sincerely,

Susan M. Collins

Chairman

Robert P. Casey, Jr.

Ranking Member

Executive Summary

From January 1, 2017, through December 31, 2017, the Senate Aging Committee's Fraud Hotline received a total of 1,463 complaints from residents all across the country. Calls pertaining to the top 10 scams featured in this report accounted for more than 75 percent of the complaints.

The top complaint, the focus of more than twice as many calls as any other scam, involves seniors who receive calls from fraudsters posing as agents of the Internal Revenue Service (IRS). These criminals falsely accuse seniors of owing back taxes and penalties in order to scam them. Due to the extremely high call volume and continued reports from constituents from across the country, the Aging Committee held a hearing on April 15, 2015, to investigate and raise awareness about the IRS imposter scam. Prior to a large law enforcement crackdown in October 2016, 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 into the Committee's hotline dropped by an incredible 94 percent. Though the numbers have since rebounded somewhat, they are still far below the levels we have seen in the past.

The second most common scam reported to the Hotline involved robocalls or unwanted telephone calls. On June 10, 2015, the Aging Committee held a hearing on the increase in these calls that are made despite the national Do-Not-Call Registry. The Committee examined how the rise of new technology has made it easier for scammers to contact and deceive consumers and has rendered the Do-Not-Call registry ineffective in many ways. On October 4, 2017, the Aging Committee held an additional hearing on robocalls, this time examining recent developments by both the private and public sectors to combat robocalls and protect seniors from fraud.

Sweepstakes scams, such as the Jamaican lottery scam, continue to be a problem for seniors, placing third on the list. A March 13, 2013, Aging Committee hearing and investigation helped bring attention to these scams and put pressure on the Jamaican government to pass laws cracking down on criminals who convinced unwitting American victims that they had been winners of the Jamaican lottery. The United States government has had some recent success in bringing individuals connected to the Jamaican lottery scam to trial, but these types of scams continue to plague seniors.

A new scam to make the top 10 list for 2017 involves consumers receiving calls in which the caller would simply ask "Are you there?" or "Can you hear me?" in order to prompt the recipient to say "yes." According to the Federal Trade Commission (FTC), these illegal robocalls are pre-recorded, and are designed to identify numbers that consumers are likely to answer, allowing scammers to better identify and connect with potential victims. The increased use of this tactic by scammers in robocalls last year demonstrates how sophisticated scammers are.

Grandparent scams, the focus of a July 16, 2014, Aging Committee hearing, were next on the list. In these scams, fraudsters call a senior pretending to be a family member, often a grandchild, and claim to be in urgent need or money to cover an emergency, medical care, or a legal problem.

Computer scams were sixth on the list and the subject of an October 21, 2015, Committee hearing. Although there are many variations of computer scams, fraudsters typically claim to represent a well-known technology company and attempt to convince victims to provide them with access to their computers. Scammers often demand that victims pay for bogus tech support services through a wire transfer, or, worse yet, obtain victims' passwords and gain access to financial accounts.

Romance scams were seventh on the list. These calls are from scammers who typically create a fake online dating profile to attract victims. Once a scammer has gained a victim's trust over weeks, months,

or even years – the scammer requests money to pay for an unexpected bill, an emergency, or another alleged expense or to come visit the victim – a trip that will never occur.

Elder financial abuse was eighth on the list and the topic of a February 4, 2015, Committee hearing. The calls focused on the illegal or improper use of an older adult's funds, property, or assets. Chairman Susan M. Collins, former Ranking Member Claire McCaskill, and current Ranking Member Robert P. Casey Jr. have introduced the *Senior$afe Act*, which would allow trained financial services employees to report suspected cases of financial exploitation to the proper authorities without concern that they would be sued for doing so. The Committee also examined the financial abuse of guardians and other court appointed fiduciaries at a hearing in November 2016.

Identify theft was the ninth most reported consumer complaint to the Fraud Hotline in 2017. This wide-ranging category includes calls about actual theft of a wallet or mail, online impersonation, or other illegal efforts to obtain a person's identifiable information. On October 7, 2015, the Aging Committee held a hearing titled *"Ringing Off the Hook: Examining the Proliferation of Unwanted Calls"*, to assess the federal government's progress in complying with a new law requiring the removal of seniors' Social Security numbers from their Medicare cards, which will help prevent identity theft. Medicare will start mailing the new cards in April 2018.

Government grant scams rounded out the top 10 scams to the Fraud Hotline last year. In these scams, thieves call victims and pretend to be from a fictitious "Government Grants Department." The con artists then tell the victims that they must pay a fee before receiving the grant.

2017 Key Figures

Rank	Type of Scam	# of Complaints
1	IRS Impersonation Scams	381
2	Robocalls / Unsolicited Phone Calls	166
3	Sweepstakes / Jamaican Lottery Scam	111
4	"Can you hear me?" Scam	97
5	Grandparent Scam	87
6	Computer Scam	79
7	Romance Scam	64
8	Elder Financial Abuse	51
9	Identity Theft	40
10	Government Grant Scam	37

Figure 1. Top 10 Scams Reported To Aging Committee Fraud Hotline from January 1, 2017, to December 31, 2017.

Figure 2. Origin of Calls Received by the Aging Committee Fraud Hotline from January 1, 2017, to December 31, 2017.

Abbreviations

Adult Protective Services	**APS**
Better Business Bureau	**BBB**
Department of Homeland Security	**DHS**
Department of Justice	**DOJ**
Federal Communications Commission	**FCC**
Federal Trade Commission	**FTC**
Financial Industry Regulatory Authority	**FINRA**
Government Accountability Office	**GAO**
Health insurance claim number	**HICN**
Internal Revenue Service	**IRS**
Internet Crime Complaint Center	**IC3**
Legal Services for the Elderly	**LSE**
Private Debt Collection	**PDC**
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 2.1 million Americas have been targeted by scammers impersonating IRS officials.[2] More than 12,300 Americans have lost a total of more than $64.9 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 a week.[4] The IRS impersonation scam was the most frequent scam reported to the Committee's Fraud Hotline for the past three 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 a difference and harder from 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' 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.

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 a 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

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.

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 cancelled.

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 victims remains hooked, the scammers will tell them they owe more money.

These scams 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, DC, 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 areas 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 January 2018, TIGTA and the Department of Justice (DOJ) have obtained 62 convictions for individuals involved in IRS impersonation scams, up from just five convictions a year ago.[11] In 2016, TIGTA and DOJ began making progress in arresting and charging more criminals for their role in this pervasive scam.

Because of a tip reported to the Committee's Fraud Hotline, in May 2016, TIGTA arrested 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.[12] 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 identity and indict 10 additional suspects who were involved in the impersonation scam.[13] To date, the teams developed evidence and established the 15 indicted individuals victimized nearly 8,000 people and stole approximately $9,000,000 from the victims.[14]

Fraud Case #1:

"Sharon," from Texas, called the Fraud Hotline to report that she lost $21,000 to the IRS Impersonation Scam. Sharon said she received a call from someone claiming to work for the IRS. The alleged scammer directed her to send several electronic money transfers in various amounts until the "outstanding debt" was paid off. A Fraud Hotline investigator filed a report with TIGTA and the FTC. Sharon was also encouraged to report this scam to her local police department.

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 has 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

Fraud Case #2:

"Sue" from Michigan, called the Fraud Hotline to report that she had fallen victim to the IRS impersonation scam. Sue said she had paid the scammers using iTunes gift cards which she purchased at a grocery store. In all, Sue bought $12,000 worth of gift cards. After purchasing the gift cards, Sue read the numbers on the back of the cards to the person on the phone whom she believed was an IRS agent. This allowed the scammer to steal the funds on the cards. Sue did not realize she had been scammed until later in the day when she told her friend about the phone call. A Fraud Hotline investigator filed a report with TIGTA and the FTC on her behalf.

wire transfer to Minnesota and reported this information to TIGTA. TIGTA sent agents to Minnesota, pulled surveillance tapes, and quickly identified three additional suspects.[15] Law enforcement arrested all give suspects and subsequently charged them with wire fraud[16] and conspiracy to commit wire fraud. At the time, this was the largest single law enforcement action in the history of the IRS impersonation scam.[17]

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.[18] Following this crack down, 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 15 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.[19] During the second week of January 2017, TIGTA reported that it received just eight new reports of victims losing money to this scam.[20] TIGTA believes this substantial drop-off is due, in part, to the October 2016 indictments of Indian call center operators.

Cumulative IRS Impersonation Scam Dollar Loss

$64,927,461 Total Dollar Loss as of January 31, 2018 ($768,901 have no state associations)

The Committee's own data show that these arrests had 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. Though the numbers have since rebounded somewhat, they are still far below the levels we have seen in the past. On October 4, 2017, Genie Barton, the President of the Better Business Bureau's Institute for Marketplace Trust, testified before the Senate Aging Committee's hearing titled, "*Still Ringing Off the Hook: An Update on Efforts to Combat Robocalls*, that her organization saw a similar trend. According Ms. Barton, the Better Business Bureau's Scam Tracker saw an immediate 95 percent drop in reports of tax collection scams following the arrests in India.[21] Ms. Barton adds that while the volume of tax scams has since risen, the volume is only 30 percent of what the volume was at the scam's peak in 2016.

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 was a naval officer and served 23 years in the Navy, described feeling both mad and upset that he had been scammed by these criminals.

Besides the arrests made in early 2017 in relation to the tip provided by the Senate Aging Committee, on November 30, 2017, TIGTA and the DOJ announced that four individuals had been arrested for their alleged involvement in the IRS impersonation scam. According to the criminal complaint, the individuals were "runners" who used fraudulent identification cards to pick up fraud proceeds sent by victims all across the country.[22] According to the complaints, the individuals picked up $666,537 sent from 784 victims during the period from January 25, 2016, through August 8, 2017.[23] The false identities used by the individuals were linked to an additional 6,530 fraudulent transactions totaling $2,836,745.[24] The individuals were charged with wire fraud, conspiracy to commit wire fraud, and aiding and abetting.[25] Each of these charges carries a maximum of 20 years imprisonment and a $250,000 fine.[26]

Beginning in April 2017, the IRS began doing something 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.[27] Once the IRS sends its letter, the private company will send its own letter and then may begin calling the taxpayer.[28]

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.[29]

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) to 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 as from scams and identify 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.

The IRS released the following tips to help taxpayers identify suspicious calls that may be associated with the IRS imposter 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 specific payment method for taxes, such as a prepaid debit card.

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.[30] Unfortunately, after 14 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.[31] To demonstrate the growing problem, in 2016, the Federal Trade Commission (FTC) received more than 3.4 million robocall complaints. In 2017, the FTC received more than 3.5 million robocall complaints within the first eight months.[32]

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

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.

Robocalls have become an interesting nuisances to consumers in recent years due to advances in technology. Phone calls used to be routed though equipment that was costly and complicated to operate, which made high-volume 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.

Many companies now offer third-party spoofying 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*

Voice over Internet Protocol (VoIP) is a technology that allows a caller to make voice calls using a broadband Internet connection 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.

Fraud Case #4:

"Stuart," from Virginia, called the Fraud Hotline to report a large number of telemarketing and soliciting phone calls including some that were "obviously" scams. Stuart described receiving calls about an expired warranty on his vehicle, when its 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.

Proliferation of Unwanted Calls".[33] 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, discussed how advanced in telephone technology makes it easier for scammers to case a wide net and increase the number of potential victims they can reach, and highlighted possible technological solutions to this menace.[34]

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 been 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.[35]

In 2016, the FCC convened a "Robocall Strike Force" comprised of telecom and tech company representatives to accelerate the

Fraud Case #5:

"Kate," from New York, contacted the Fraud Hotline to report receiving unsolicited phone calls that show up as "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 directed to contact her local telephone company and inquire about call blocking features.

Fraud Case #6:

"Al," from Arizona, called to report receiving a sweepstakes scam call. The caller told Al that he had won $1 million, but would need to pay $200 in iTunes gift cards to receive his prize. After purchasing the gift card, Al read the numbers on the back of the cards to the person on the phone. This allowed the scammer to steal the funds off the card. The Fraud Hotline investigator filed a report with the Federal Trade Commission and the Department of Homeland Security.

development and adoption of new tools to combat illegal robocalls.[36] 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, 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.[37]

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.[38] The Commission voted to finalize new rules to allow phone companies to block certain phone numbers that do not or cannot make outgoing calls.[39] 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 company but haven't 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 identity innovative solutions to protect consumers from these calls.[40] 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 their Robocall Challenge.[41]

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.[42] If the caller is one 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 feedback from callers who chose to register for the service.

In the spring of 2015, the FTC announced that it was launching two new robocall contests challenging the public to develop a crowdsourced "honeypot" and to better analyze data from an existing honeypot.[43] In this context, a honeypot is an information system that attracts robocalls so that researchers can analyze them and develop preventive techniques.[44] 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.[45] 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.[46]

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 aa 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 Scam

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.[47] According to the Federal Trade Commission (FTC), the number of sweepstakes scams increased by 44.5 percent between 2013 and 2016.[48,49] 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".[50]

During the 113th Congress, the Aging Committee launched an investigation of the Jamaican lottery scam, one of the most pervasive sweepstakes scams.[51] 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.[52]

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

Sweepstakes scams start with a simple phone call, usually 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 the money in a variety of ways, including prepaid debit card, electronic wire transfers, money orders, and even cold hard cash.

Fraud Case #7:

"Vickie," from Pennsylvania, called the Fraud Hotline to report a sweepstakes scam from a company, which had no name. They told her she was a recipient of a $1 million prize, but would have to wire $500 via Western Union. Knowing this was not real, she hung up the phone and called the police. A Fraud Hotline investigator filed a complaint to the FTC on her behalf.

Of course, no such winnings are ever delivered, and the "winners" get nothing but 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.[53] Criminals once involved in narcotics trafficking have found these scams to be safer and more lucrative.

Fraud Case #8:

"Kelly," from Connecticut, called the Fraud Hotline to report that her grandmother lost $200 in a sweepstakes scam. The scammer claimed to be various people, but did not associate with any organization. She was told she won $1 million and a brand new car. A Fraud Hotline investigator filed a report with the electronic wire transfer company, the Federal Trade Commission, and the Department of Homeland Security. The investigator also sent Kelly additional information on the sweepstakes scam to share with her grandmother.

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.[54] 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."[55]

Expensive "lead lists" identify potential victims. Satellite maps are used to locate and describe 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, Secretary of State Rex Tillerson noted the important progress Jamaica was making combatting lottery scams, including cooperating closely with the United States to extradite suspected lottery scammers and for establishing a bilateral lottery scam task force.[56] As Secretary Tillerson noted, it is in both countries' interests to work together to investigate crimes, share intelligence, conduct asset seizures where legally and appropriate to do so, and bolster existing anti-corruption and anti-gang programs.[57]

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 "Can You Hear Me?" Scams

In early 2017, consumers began reporting receiving calls in which the caller would simply ask "Are you there?" or "Can you hear me?" in order to prompt the recipient to say "yes." Within just the first few months of 2017, the Federal Trade Commission (FTC) had already received hundreds of complaints about these calls.

After responding, "yes," consumers would often report that the call would immediately drop, or get disconnected. As a result, the immediate concern was that scammers would record the consumer's voice, and thus obtain a voice signature, and use the recording to authorize unwanted charges on items like utility bills, phone bills, or even stolen credit cards.[58]

In February 2017, a man from Washington claimed there was an unauthorized $100 charge on his credit card, one day after saying "yes" to someone on the phone who asked, "Hello, hello, can you hear me?" The caller describes that once he said yes, the caller began to pitch a resort vacation package. When the victim challenged the caller, the caller immediately hung up. A few days later, the victim, not yet knowing that he had been defrauded, read about the "Can you hear me?" scam, and immediately checked his credit card statement. The victim noticed an unauthorized charge of $100.79 for a hotel room, less than 24 hours after he received the "Can you hear me?" call. The victim's credit card company reversed the charge when he filed a fraud report.

Fraud Case #9:

"Cindy," from Pennsylvania called the Fraud Hotline to report receiving a call from someone who asked her, "Can You Hear Me?" Cindy was scared and contacted her bank and local police department. A Fraud Hotline investigator filed a report with the Federal Trade Commission and encouraged her to monitor her accounts and not to answer any call she doesn't recognize.

Only a few consumers have reported losing money to this scam. On October 4, 2017, Genie Barton, the President of the Better Business Bureau's Institute for Marketplace Trust, testified before the Senate Aging Committee's hearing titled, "*Still Ringing Off the Hook: An Update on Efforts to Combat Robocalls*, that out of the 10,000 published "Can you hear me?" reports, fewer than 20 involved a reported dollar loss, and those losses cannot be definitively connected to a "yes" response.[59] The fact that more people were not reporting a monetary loss caused consumer protection advocates and law enforcement agencies to believe that these calls were not being placed to scam people out of their money, but to help identify active phone numbers and thus increase the odds of being able to scam a victim.

According to the FTC, these illegal robocalls are originated by recordings,[60] and are designed to identify numbers that consumers are likely to answer.[61] The FTC believes that the "Can you hear me?" recording may act as a sort of filler.[62] Instead of music, or dead air, the recording may be a filler waiting for a live telemarketer to free up and actually get on the call.[63] In addition, the FTC believes that if the recipient of the call answers "yes," the calls are then automatically transferred to a live scammer or telemarketer.[64] A staggering 34 percent of all published reports to the Better Business Bureau's Scam Tracker in the first half of 2017 regarding robocalls can be classified as robocalls.[65] The increased use of this tactic by scammers last year demonstrates how sophisticated these scammers are and the success it could have in helping scammers better identify and connect with likely victims.

The Federal Trade Commission (FTC) has published the following tips for consumers who get a call from someone they don't recognize asking, "Can you hear me?":

- Don't respond, just hang up. If you get a call, don't press 1 to speak to a live operator or any other number to be removed from the list. If you respond in any way, it will probably just lead to more robocalls – and they're likely to be scams.
- Contact your phone provider. Ask your phone provider what services it provides to block unwanted calls.
- Put your phone number on the Do Not Call registry. Access the registry online or by calling 1-888-382-1222. Callers who don't respect the Do Not Call rules are more likely to be crooks.
- File a complaint with the FTC. Report the experience online or call 1-877-382-4357.

Source: https://www.consumer.ftc.gov/blog/2017/03/calls-asking-can-you-hear-me-now

5 Grandparent Scams

A common scam that deliberately targets older Americans is the "grandparent scam." In this scam, imposters either pretend to be the victim's grandchild and/or claim to be holding the victims' grandchild. The fraudsters claim the grandchild is in trouble and needs money to help with an emergency, such as getting out of jail, paying a hospital bill, or leaving a foreign country. Scammers play on victims' emotions and trick concerned grandparents into wiring money to them. Once they money is wired, it is difficult to trace. For example, last summer 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.[66]

Fraud Case #10:

"Bob," from Florida, called the Fraud Hotline to report losing $6,000 to a grandparent scam. Bob received a call from someone claiming to be his grandson, saying he had been in an accident. The caller instructed Bob to purchase iTunes gift cards. After purchasing them, Bob read the numbers on the back of the cards to the person on the phone. This allowed the scammer to steal the funds off the card. Bob became suspicious when the person on the phone began requesting more money. The Fraud Hotline investigator filed a report with the Federal Trade Commission on his behalf and sent him a copy of the Fraud Book.

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. 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 more money is needed. Scammers often claim that there was another legal fee they were not initially aware of. 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 they had asked the con artists some simple questions that only their true grandchild would know how to answer.

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 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 they victim will recognize that the voice on the phone does not belong to their grandchild.

In 2016, the Federal Trade Commission (FTC) received 14,898 complaints of individuals impersonating friends and family members, up from 12,404 in 2013.[67],[68] 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.[69]

Fraud Case #11:

"Molly," from Mississippi, called the Fraud Hotline to report losing $3,800 in a grandparent scam. Molly received a call from someone claiming to be her grandson who told her that he had been arrested in the Dominican Republic and needed bail money. Among other things, the scammer requested $1,860 for an appearance bond and $900 to pay a fine for negligence. In the end, Molly ended up paying approximately $3,800 via electronic wire transfers at Western Union. The Fraud Hotline investigator filed a report Western Union and with the Federal Trade Commission.

6 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.[70] The company estimated that 3.3 million Americans are victims of technical support scams annually, with losses of roughly $1.5 billion per year.[71] Unlike other victim-assisted frauds, where the scammers are successful in just one out of a hundred-plus attempts, it appears that computer-based scams have a very high success rate.[72] In 2016, the Internet Crime Complaint Center (IC3), a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center, received 10,850 tech support fraud complaints with losses in excess of $7.8 million.[73] The IC3, noted that while fraud affects victims of all ages, older victims are often the most vulnerable.[74]

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*".[75] The hearing featured representatives from Microsoft and the FTC who spoke about the challenges in combatting this fraud given its many variations and constant changes.[76]

The basic scam involves con artists trying to gain 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 credit card and bank account numbers so that victims can be "billed" for fraudulent services to fix the virus. In a related scam, individuals surging 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.

Fraud Case #12:

"Brian," from Georgia, called the Fraud Hotline to report that he had fallen victim to a tech support scam. Brain explains that a pop-up appeared on his computer screen that would prevent him from doing anything. The pop-up was masking itself as a Microsoft dialogue box and informed him to call a number to get a virus removed. The first couple of times it appeared, Brian would restart his computer, but he eventually called the number on the dialogue box. The person on the phone identified himself as "Cam" from "US Infotech" in Texas. The scammer told Brain that his computer was infected with a virus and that he would need to take control of his computer to clean it and install anti-virus software. Brian paid the scammers $895 in "service fees, software, and damage repair costs" using his credit card. The Fraud Hotline investigator encouraged Brian to dispute the charge with his credit card company, and filed a report with the Federal Trade Commission and the FBI's Internet Crime Complaint Center on his behalf.

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

- **Scammers Contact Victims.** In the most prevalent variation of this scam, con artists randomly call potential victims and offer to clean their computers and/or sell them a long-term or technical support "service". The con artist usually direct victims' computers to display benign error messages that appear on every computer to convince victims that their computers are malfunction. 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."

- **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 and for certain key search terms.[77] 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 re associated with well-known companies. Other fraudsters use pop-up messages on consumers' computer screens that direct potential victims to call them.

- **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, scammer's 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.

- **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.

Fraud Case #13:

In October 2015, Frank Schiller, from Maine, testified at an Aging Committee hearing on computer tech support scams. Frank's experience with tech support scammers began in October 2013, when he received a call from a man who claimed to be a Microsoft contractor. The con artist told Frank there was a problem with his computer. He gained Frank's trust and convinced Frank to allow him to obtain remote access to his computer. Shortly thereafter, Frank's computer began to malfunction, and the con artist explained that this was due to viruses that "Microsoft" could fix using two programs costing $249 and $79. Frank attempted to pay for these programs using his credit card, but the scammer told him that he could not use a credit card because Microsoft's bank was in India. The con artist directed Frank to the Western Union website and moved very quickly through the payment system before Frank could tell what was happening. Two months later, the con artist called Frank again to say that Microsoft had rescinded his contract and would need to refund Frank's money. The con artist claimed that the refund could not be processed using Frank's credit card and asked for his checking account number. This information was used to steal another $980 from Frank.

The FTC has responded to computer-based scams through law enforcement actions and ongoing investigations. In 2014, the agency brought action against six firms based primarily in India that were responsible for stealing more than $100 million from thousands of victims.[78]

On May 12, 2017, the Department of Justice announced that seven individuals were charged for their participation in the tech support scam.[79] Seven individuals received criminal indictments for their role in the Florida-based Client Care Experts 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.[80] These pop-ups falsely informed the victims that serious problems, such as viruses or malware, had been detected on their computers.[81] 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.[82]

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.

Source: http://www.consumer.ftc.gov/articles/0346-tech-support-scams

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.[83] 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 up, this is up from just six percent back in 2013.[84]

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 artist gain the trust of victims 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, 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.[85] Con artists have been known to create elaborate profile pages, giving their fabricated story more credibility. Con artist often call and chat on the phone to prove that they are real. These conversation can take place over weeks and even months as the con arts build trust with their victims. In some instances, con artist have even promised to marry their victims.

Fraud Case #14:

"Linda," from California, called the Fraud Hotline on behalf of her sister who was in the midst of a romance scam. According to Linda, her sister had sent $729,500 over the span of two years to a scammer she met on an online dating website. She had been directed to send the money through her bank in wire transfers. The Fraud Hotline investigator filed a report with the Federal Trade Commission, the FBI's Internet Crime Complaint Center, and the Secret Service. Linda was also encouraged to report this crime to the California Attorney General's office and to her sister's local police department. The investigator also sent Linda additional information about this type of scam to share with her sister.

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 other relative, visas or other official documents, or losses from a temporary financial setback.[86] 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.[87]

In 2016, the FBI's IC3 received 14,546 complaints about romance and confidence scams that cost victims $219,807,706, the second highest type of scam by victim loss reported to the IC3.[88] In comparison, in 2014, the IC3 received 5,883 complaints about romance and confidence scams that cost victims $86.7 million dollars.[89] 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 last year.[90] Romance and confidence scams disproportionally target women, usually between the ages of 30 and 55 years old.[91] Unfortunately, both the amount of financial loss and the number of complaints for the crime have increased in recent years.[92]

Tips 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 Elder Financial Abuse

Financial exploitation of older Americans is the illegal or improper use of an older adult's funds, property, or assets. According to MetLife's Mature Market Institute, in 2010 seniors lost an estimated $2.9 billion because of financial exploitation, $300 million more than the year before, although these numbers are likely substantially underreported.[93] One study found that, for every case of financial fraud that is reported, as many as 14 go unreported.[94]

A 2011 Government Accountability Office (GAO) study found that approximately 14.1 percent of adults age 60 and older experienced physical, psychological, or sexual abuse; potential neglect; or financial exploitation in the past year.[95]

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.[96] APS can also refer cases to law enforcement agencies or district attorneys for criminal investigation and prosecution.[97] 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.[98]

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.[99] Most victims are between the ages of 80 and 89, live alone, and require support with daily activities.[100] Perpetrators include family members; paid home care workers; those with fiduciary responsibilities, such as financial advisors or legal guardians or strangers who defraud older adults through mail, telephone, or Internet scams.[101]

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.[102] Few civil attorneys, however, are trained in issues related to older victims and financial exploitation.[103] 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.[104]

One of the provisions of the Elder Justice Act of 2009, which was enacted in 2010, seeks to improve the federal response to this issue.[105] The law formed the Elder Justice Coordinating Council, which first convened on October 11, 2012, and is tasked with increasing cooperation among federal agencies.[106] 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.[107]

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

Fraud Case #15:

"Glen," from Oregon, called the Fraud Hotline to report that his mother-in-law had become the victim of elder financial abuse before her death. Glen describes that a caretaker for his mother-in-law got control of her retirement fund which was valued at $200,000. A Fraud Hotline investigator shared information with Glen about elder financial exploitation and encouraged him to file a complaint with the Oregon Attorney General's office.

professionals may fail to report suspected financial exploitation due to a lack of training or fear of repercussions for violating privacy laws. Aging Committee Chairman Susan Collins and former Ranking Member Claire McCaskill have introduced the Senior Safe Act, a bipartisan bill cosponsored by Ranking Member Robert P. Casey Jr. and others, which would provide certain individuals with immunity for disclosing suspected financial exploitation of senior citizens.[108] The Financial Regulatory Authority is simultaneously pursuing rulemaking that would empower financial professionals to protect their senior clients from financial abuse.[109]

Some localities with large senior populations have established special units to address elder abuse, including elder financial abuse. In October 2015, prosecutors in Montgomery County, Maryland, successfully brought charges against an individual who, over several years, embezzles more than $400,000 before one of the victim's bankers discovered suspicious activity in his account and alerted APS.[110] 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.[111]

In March 2016, an attorney in Belfast, Maine was sentenced to 30 months in prison for bilking two elderly female clients out of nearly a half of a million dollars over the course of several years.[112] 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.[113] When confronted by authorities, he offered excuses that the prosecutor later described as "breathtaking."[114] For example, according to the *Bangor (Maine) Daily News,* he put one of his clients into 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.[115]

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.[116] 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, cheated her of an estimated $1 million in assets.[117] 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.[118]

The Aging Committee has brought to light many schemes that have defrauded seniors out of their heard-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. During the hearing, titled, *"Trust Betrayed: Financial Abuse of Older Americans by Guardians and Others in Power"*, the Committee released a new GAO report on guardianship abuse. The report builds on a 2010 study which found hundreds of cases of abuse, neglect, and exploitation and identified $5.4 million that had been improperly diverted.[119] The updated report examined cases of elder financial abuse over a four-year period, from 2011 to 2015, and examined measured taken by several states to help protect older adults with guardians.

According to the GAO, guardianship abuse is widespread, but it remains difficult to determine the extent of elder abuse by guardians nationally due to limited data. GAO noted that 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 has 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 education 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 software0based system that scams 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 system available to other states free of change.

Another witness, Jaye Martin, the Executive Director of Legal Services of the Elderly (LSE) in Maine, testified that her organization assisted 260 victims of elder abuse during the last 12 months. 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 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 only represent the tip of the iceberg, since so many abuses cases go unreported. Victims are often ashamed or afraid to alert authorities about financial exploitation, particularly when it involves a family member.

9 Identity Theft

Identity thieves not only disrupt the lives of individuals by draining bank accounts, marking 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 an 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 most common type of consumer complaint in 2016, with 399,225 complaints.[120]

For the first time in 15 years, however, identify theft was not the FTC's most common consumer complaint in 2015. Even so, 490,220 Americans still reported being victimized.[121] Consumers age 50 and older reported 45 percent of the identity theft complaints that the FTC received in 2015.[122]

The growing use of commercial tax filing software and online tax filling 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, e-mail address, or name and correctly guessing the 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 file his 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 with copies of the fake retuned upon written request.[123] 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.[124] According to the IRS, the number of people reporting stolen identities on federal tax retuned fell by more than 40 percent, with nearly 242,000 fewer victims compared to a year ago.[125]

Fraud Case #16:

"Rob," from Iowa, called the Fraud Hotline because he believed his father was the victim of identity theft. Rob explains that his father began receiving multiple collection notices about credit cards that apparently were opened in his name. The Fraud Hotline investigator gave Rob information on how to file a credit freeze and to dispute the transactions.

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 rating, and waste taxpayer dollars. Some identity theft can disrupt lives, damage credit ratings, and waster taxpayer

dollars. Some identify thieves 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 might be included in the beneficiary's Medicare billing history and could 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.[126] Medicare is mailing new Medicare cards to all people beginning in April 2018.[127] On October 7, 2015, the Aging Committee held a hearing titled, "*Protecting Seniors from Identity Theft: Is the Federal Government Doing Enough*".[128] 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.[129]

The 2017 Equifax data breach may have exposed private information belonging to 145.5 million people — nearly half of the U.S. population.[130] The Senate Aging Committee 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 the 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 to 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.[131] 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 from 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 on 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.[132] The scammer also tried to get the consumer's sensitive personal information, including full name and Social Security number.

Fraud Case #17:

"Diane," from Maine, called the Fraud Hotline to inquire about how to freeze her credit in light of the recent Equifax data breach. A Fraud Hotline investigator gave Diane information about identity theft and how to place a credit freeze.

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

Source: https://www.identitytheft.gov

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 FTC.
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.

Tips to Help Secure Your Identity:

- Neither Medicare nor Social Security will call 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 to someone you do not know.
- 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.

10 Government Grant Scams

Grant scams, of which there are multiple variations, are frequently reported to the Senate Aging Committee's Fraud Hotline. In the most common variation of this scam, consumers receive and unsolicited phone call from con artists claiming that they are from the "Federal Gants Administration," or the "Federal Grants Department" – agencies that do not exist. In another version of this scam, scammers place advertisements in the classified section of local newspapers offering "free grants," and will request that victims wire money for processing fees or taxes before the money can be sent to them.

The Federal Trade Commission (FTC) defines grant scams as, "[deceptive practices by businesses or individuals marketing either government grant opportunities or financial aid assistance services; problems with student loan processors, debt collectors collecting on defaulted student loans, diploma mills; and other unaccredited educational institutions, etc." [133] According to FTC data, the frequency of Americans reporting grant scams has dropped over the past three years.[134] In 2016, the FTC received 4,969 complaints, which is almost a 22 percent increase from the previous year.[135,136]

Fraud Case #18:

"Deb," from Ohio, called the Fraud Hotline to report losing $245 in a government grant scam. Deb described receiving a call from someone named "Max Fletcher" who told her she won a grant for $9,000 from the "Washington Money Fund." In order to collect the funds, she was instructed to wire $250 to cover processing fees. She realized this was a scam once the scammers demanded more money for "additional unforeseen fees." Deb said this was a huge financial mistake as she only receives $855 per month on disability. A Fraud Hotline investigator filed a report with the electronic transfer company and the Federal Trade Commission.

The National Consumers League has published the following tips for consumers to avoid falling victim to a federal grant scam:

- Do not give out your bank account information to anyone you do not know. Scammers pressure people to divulge their bank account information so that they can steal the money in the account. Do not share bank account information unless you are familiar with the company and know why the information is necessary.
- Government grants are made for specific purposes, not just because someone is a good taxpayer. They also require an application process; they are not simply given over the phone. Most government grants are awarded to states, cities, schools, and nonprofit organizations to help provide services or fund research projects. Grants to individuals are typically for things like college expenses or disaster relief.
- Government grants never require fees of any kind. You might have to provide financial information to prove that you qualify for a government grant, but you never have to pay to get one.

Source: http://www.fraud.org/scams/telemarketing/government-grants

Conclusion

One of the Senate Aging Committee's top priorities in the 115th Congress is to continue combatting fraud that targets seniors. The Fraud Hotline has been instrumental in this fight, providing more than 1,400 people in 2017 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 consumers. 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. For example, in November 2017, AARP released a report that found that military veterans are more likely than other Americans to be victims of scams and that some scams are specifically aimed at programs and charities geared to veterans.[137]

As the Aging Committee enters the second session of the 115th 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 and to encourage a more effective federal response to these scams.

This Fraud Book is designed 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, contact the Aging Committee's Fraud Hotline at **1-855-303-9470**.

Top Scams by State

These scams are based on calls into the Aging Committee's Fraud Hotline in 2017.

Alabama

1. IRS Impersonation Scam
2. Unsolicited Phone Calls
3. Grandparent Scam
4. Romance Scam
5. Identity Theft

Alaska

1. IRS Impersonation Scam
2. Grandparent Scam

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

Arizona

1. IRS Impersonation Scam
2. Grandparent Scam
3. Romance Scam
4. Unsolicited Phone Calls
5. "Can You Hear Me?" Scam

Arkansas

1. IRS Impersonation Scam
2. Romance Scam
3. Impending Law Suit Scam
4. IRS Fraudulent Tax Returns

California

1. IRS Impersonation Scam
2. Elder Financial Abuse
3. Romance Scam
4. Unsolicited Phone Calls
5. "Can You Hear Me?" Scam

Colorado

1. IRS Impersonation Scam
2. Computer Tech Support Scams
3. Romance Scams
4. "Can You Hear Me?" Scam
5. Debt Collection Scams

Connecticut

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

Delaware

1. IRS Impersonation Scam

Florida

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

Georgia

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

Hawaii

1. IRS Impersonation Scam
2. Government Grant Scams

Idaho

1. Identity Theft
2. IRS Impersonation Scam
3. Romance Scams

Illinois

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

Indiana

1. Unsolicited Phone Calls
2. Grandparent Scams
3. Computer Tech Support Scams
4. Impending Law Suit Scams
5. Social Security Fraud

Iowa

1. Unsolicited Phone Calls
2. Identity Theft
3. Inheritance Scams

Kansas

1. Romance Scams
2. Mortgage Fraud

Kentucky

1. IRS Impersonation Scam
2. Computer Tech Support Scams
3. Romance Scams

Louisiana

1. IRS Impersonation Scam
2. Romance Scams
3. “Can You Hear Me?” Scam
4. Elder Financial Abuse

Maine

1. IRS Impersonation Scam
2. “Can You Hear Me?” Scam
3. Unsolicited Phone Calls
4. Grandparent Scam
5. Computer Tech Support Scams

Maryland

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

Massachusetts

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

Michigan

1. IRS Impersonation Scam
2. Computer Tech Support Scams
3. Romance Scams
4. Unsolicited Phone Calls
5. “Can You Hear Me?” Scam

Minnesota

1. IRS Impersonation Scam
2. Romance Scams
3. Unsolicited Phone Calls
4. Counterfeit Check Scams
5. Timeshare Scams

Mississippi

1. IRS Impersonation Scam
2. Grandparent Scam
3. Elder Financial Abuse

Missouri

1. IRS Impersonation Scam
2. Identity Theft
3. Grandparent Scams
4. Government Grant Scams

Montana

1. IRS Impersonation Scam

Nebraska

1. Elder Financial Abuse
2. Legal Referral

Nevada

1. IRS Impersonation Scam
2. Government Grant Scam
3. Debt Collection Scam
4. IRS Fraudulent Tax Returns
5. Investment Fraud

New Hampshire

1. Unsolicited Phone Calls
2. Debt Collection Scams

New Jersey

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

New Mexico

1. Computer Tech Support Scams

New York

1. IRS Impersonation Scam
2. Unsolicited Phone Calls
3. Computer Tech Support Scams
4. Grandparent Scams
5. “Can You Hear Me?” Scam

North Carolina

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

North Dakota

1. Unsolicited Phone Calls

Ohio

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

Oklahoma

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

Oregon

1. Elder Financial Abuse
2. Impending Law Suit Scams
3. Unsolicited Phone Calls
4. Identity Theft
5. Computer Tech Support Scams

Pennsylvania

1. IRS Impersonation Scam
2. Unsolicited Phone Calls
3. Wire Fraud
4. Elder Financial Abuse
5. Computer Tech Support Scams

Rhode Island

1. IRS Impersonation Scam
2. Unsolicited Phone Calls
3. Romance Scams
4. Grandparent Scams
5. IRS Fraudulent Tax Returns

South Carolina

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

South Dakota

1. Grandparent Scams
2. Unsolicited Phone Calls

Tennessee

1. IRS Impersonation Scam
2. Grandparent Scams
3. Identity Theft
4. Investment Fraud
5. Unsolicited Phone Calls

Texas

1. IRS Impersonation Scam
2. Romance Scams
3. Grandparent Scam
4. Computer Tech Support Scam
5. Government Grant Scam

Utah

1. IRS Impersonation Scam
2. Grandparent Scam
3. Unsolicited Phone Calls
4. “Can You Hear Me?” Scam
5. Timeshare Scams

Vermont

1. IRS Impersonation Scam

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

Virginia

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

Washington

1. IRS Impersonation Scam
2. Unsolicited Phone Calls
3. Grandparent Scam
4. Romance Scams
5. Investment Fraud

West Virginia

1. IRS Impersonation Scam
2. Elder Financial Abuse
3. Robbery / Theft

Wisconsin

1. IRS Impersonation Scam
2. Grandparent Scam
3. Elder Financial Abuse
4. Identity Theft

Wyoming

1. IRS Impersonation Scam

Appendix 1: 2017 Complete Aging Fraud Hotline Statistics

Scam Type	Total
IRS Scam	381
Unsolicited Phone Calls	166
Sweepstakes / Jamaican Lottery Scam	111
Can You Hear Me? Scam	97
Grandparent Scam	87
Computer Scam	79
Romance Scam	64
Elder Abuse	51
Identity Theft	40
Government Grant	37
Impending Law Suits	37
Wire Fraud	28
Mail Scam	22
Health-Related Scam	21
Check Scam	19
Debt Collection Scam	13
IRS Fraudulent Tax Returns	10
Investment Fraud	9
Utility Scams	9
Mortgage Fraud	8
Timeshare Scam	6
Social Security Fraud	5
Spam Email	5
Charity Scam	4
Home Improvement Scam	4
Legal Referral	4
Pension/Retirement Savings Fraud	2
Unclaimed Property Scam	2
Bank Fraud	1
Grand Jury Impersonation Scam	1
Inheritance Scam	1
Payday Lending	1
Robbery/Theft	1
Miscellaneous**	137
TOTAL	**1463**

Origin of Call	Total
Alabama	11
Alaska	0
Arizona	36
Arkansas	12
California	66
Colorado	8
Connecticut	14
Delaware	4
Florida	79
Georgia	14
Hawaii	3
Idaho	3
Illinois	31
Indiana	20
Iowa	6
Kansas	2
Kentucky	11
Louisiana	5
Maine	521
Maryland	62
Massachusetts	12
Michigan	21
Minnesota	8
Mississippi	5
Missouri	9
Montana	1
Montana	4

Origin of Call	Total
Nebraska	3
Nevada	6
New Hampshire	3
New Jersey	22
New Mexico	1
New York	61
North Carolina	12
North Dakota	6
Ohio	24
Oklahoma	8
Oregon	11
Pennsylvania	162
Rhode Island	8
South Carolina	15
South Dakota	3
Tennessee	15
Texas	60
Utah	9
Vermont	0
Virginia	23
Washington	13
West Virginia	6
Wisconsin	10
Wyoming	1
Unknown	17
Wyoming	2

Appendix 2: Aging Committee's Top 10 Historical Data

2017 Rank	Type of Scam	2015	2016	2017
1	IRS Impersonation Scam	387	1680	381
2	Robocalls / Unsolicited Phone Calls	93	92	166
3	Sweepstakes / Jamaican Lottery Scam	157	124	111
4	"Can you hear me?" Scam	** New Scam in 2017**		97
5	Grandparent Scam	63	39	87
6	Computer Scam	87	77	79
7	Romance Scam	28	36	64
8	Elder Financial Abuse	59	53	51
9	Identity Theft	75	16	40
10	Government Grant Scam	37	35	37

Appendix 3. 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 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	1800-366-4484
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
Steve Marshall
(334)-242-7300

Alaska
Jahna Lindemuth
(907)-269-5100

Arizona
Mark Brnovich
(602)-542-5025

Arkansas
Leslie Rutledge
(800)-482-8982

California
Xavier Becerra
(916)-445-9555

Colorado
Cynthia Coffman
(720)-508-6022

Connecticut
George Jepsen
(860)-808-5400

Delaware
Matthew Denn
(302)-577-8600

District of Columbia
Karl A . Racine
(202)-442-9828

Florida
Pam Bondi
(850)-414-3300

Georgia
Chris Carr
(404)-656-3300

Hawaii
Douglas Chin
(808)-586-1500

Idaho
Lawrence G. Wasden
(208)-334-2400

Illinois
Lisa Madigan
(312)-814-3000

Indiana
Curtis Hill
(317)-232-6330

Iowa
Tom Miller
(515)-281-5044

Kansas
Derek Schmidt
(785)-296-3751

Kentucky
Andy Beshear
(502)-696-5300

Louisiana
Jeff Landry
(225)-326-6465

Maine
Janet T. Mills
(207)-626-8800

Maryland
Brian Frosh
(410)-576-6300

Massachusetts
Maura Healey
(617)-727-2200

Michigan
Bill Schuette
(517)-373-1110

Minnesota
Lori Swanson
(651)-296-3353

Mississippi
Jim Hood
(601)-359-3680

Missouri
Josh Hawley
(573)-751-3321

Montana
Tim Fox
(406)-444-2026

Nebraska
Doug Peterson
(402)-471-2682

Nevada
Adam Laxalt
(702)-486-3132

New Hampshire
Joseph Foster
(603)-271-3658

New Jersey
Gurbir Grewal
(609)-292-8740

New Mexico
Hector Balderas
(505)-490-4060

New York
Eric T. Schneiderman
(518)-776-2000

North Carolina
Josh Stein
(919)-716-6400

North Dakota
Wayne Stenehjem
(701)-328-2210

Ohio
Mike DeWine
(614)-466-4986

Oklahoma
Mike Hunter
(405)-521-6246

Oregon
Ellen Rosenblum
(503)-378-4400

Pennsylvania
Josh Shapiro
(701)-328-2210

Rhode Island
Peter Kilmartin
(401)-274-440

South Carolina
Alan Wilson
(803)-734-3970-

South Dakota
Marty Jackley
(605)-773-3215

Tennessee
Herbert Stlatery
(615)-741-3491

Texas
Ken Paxton
(512)-463-2100

Utah
Sean Reyes
(800)-244-4636

Vermont
TJ Donovan
(802)-828-3173

Virginia
Mark Herring
(804)-786-2071

Washington
Bob Ferguson
(360)-753-6200

West Virginia
Patrick Morrisey
(304)-558-2021

Wisconsin
Brad Schimel
(608)-266-1221

Wyoming
Peter K. Michael
(307)-777-7841

Puerto Rico
Wanda Vasquez Garced
(787)-721-2900

US Virgin Islands
Claude Earl Walker
(340)-774-5666

Appendix 4. Cut out Scam Prevention Tip Cards

Please cut out these cards and place them by your phone. Feel free to 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

References

1 U.S. Congress. Senate. 2015. Tax Schemes and Scams During the 2015 Filing Season: Hearing before the Committee on Finance. 114th Congress, 1st sess., March 12.

2 TIGTA Semiannual Report to Congress: April 1, 2017 – September 30, 2017. Pg.1 https://www.treasury.gov/tigta/semiannual/semiannual_sept2017.pdf (accessed on February 12, 2018).

3 TIGTA Email to Aging Committee. February 5, 2018.

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

5 4 U.S. Congress. Senate. 2015. *Catch Me If You Can: The IRS Impersonation Scam and the Government's Response: Hearing before the Special Committee on Aging.* 114th Congress, 1st sess., April 15.

6 Internal Revenue Service. Tax Scams/Consumer Alerts. https://www.irs.gov/uac/Tax-Scams-Consumer-Alerts (accessed January 22, 2017).

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

8 7 Internal Revenue Service. IRS Warns Taxpayers to Guard Against New Tricks by Scam Artists; Losses Top $20 Million. https://www.irs.gov/uac/newsroom/irs-warns-taxpayers-to-guard-against-new-tricks-by-scam-artists. August 6, 2015. (accessed January 22, 2017).

9 8 Internal Revenue Service. Five Easy Ways to Spot a Scam Phone Call. https://www.irs.gov/uac/Five-Easy-Ways-to-Spot-a-Scam-Phone-Call. September 2, 2014. (accessed January 22, 2017).

10 9 Treasury Inspector General for Tax Administration. IRS Impersonation Scam Update. April 21, 2016. https://www.treasury.gov/tigta/irs_scam_updates.shtml. (accessed January 22, 2017).

11 TIGTA Email to Aging Committee. February 5, 2018.

12 Associated Press. 2015. Man gets 14 years in prison for scam that took millions with fake IRS calls. *Los Angeles Times.* July 8.

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

14 Ibid.

15 Ibid

16 Ibid

17 Ibid

18 Department of Justice. Dozens of Individuals Indicted in Multimillion-Dollar Indian Call Center Scam Targeting U.S. Victims. October 27, 2016. https://www.justice.gov/opa/pr/dozens-individuals-indicted-multimillion-dollar-indian-call-center-scam-targeting-us-victims (accessed on January 25, 2017).

19 8 TIGTA Conference Call with Aging Committee. December 9, 2016.

20 TIGTA Conference Call with Aging Committee. January 22, 2017.

21 Barton, Genie. Prepared Statement of Genie Barton, President of the BBB Institute For Marketplace Trust Hearing on Robocall Scams. October 4, 2017. Pg. 11 https://www.aging.senate.gov/imo/media/doc/SCA_Barton_10_4_17.pdf (accessed on February 8, 2018).

22 United States Attorney's Office for the Eastern District of Wisconsin. *Internal Revenue Service Impersonation Scammers Arrested.* November 30, 2017. https://www.justice.gov/usao-edwi/pr/internal-revenue-service-impersonation-scammers-arrested (accessed on February 12, 2018).

23 Ibid.

24 Ibid.

25 Ibid.

26 Ibid.

27 Internal Revenue Service. *Private Debt Collection.* August 7, 2017. https://www.irs.gov/businesses/small-businesses-self-employed/private-debt-collection (accessed on February 2, 2018).

28 Ibid.

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

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

31 FCC. Notice of Inquiry. FCC 17-89. July 14, 2017. https://apps.fcc.gov/edocs_public/attachmatch/FCC-17-89A1.pdf (accessed on September 26, 2017).

32 Email from FTC to Senate Aging Committee Staff on September 28, 2017.

33 9 U.S. Congress. Senate. 2015. *Ringing Off the Hook: Examining the Proliferation of Unwanted Calls: Hearing before the Special Committee on Aging.* 114th

Congress, 1st sess., June 10.

34 Ibid.

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

36 Robocall Strike Force Report. Pg. 1 October 26, 2016. https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf (accessed on September 27, 2017).

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

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

39 Federal Communications Commission. *FCC Adopts Rules to Help Block Illegal Robocalls.* November 16, 2017. https://www.fcc.gov/document/fcc-adopts-rules-help-block-illegal-robocalls-0 (accessed on February 8, 2018).

40 Federal Trade Commission. FTC Challenges Innovators to Do Battle with Robocallers. https://www.ftc.gov/news-events/press-releases/2012/10/ftc-challenges-innovators-do-battle-robocallers October 18, 2012. (accessed January 22, 2017).

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

42 Ibid.

43 Federal Trade Commission. FTC Announces New Robocall Contests to Combat Illegal Automated Calls. https://www.ftc.gov/news-events/press-releases/2015/03/ftc-announces-new-robocall-contests-combat-illegal-automated. March 4, 2015. (accessed January 22, 2017).

44 Ibid

45 Federal Trade Commission. FTC Awards $25,000 Top Cash Prize for Contest-Winning Mobile App That Blocks Illegal Robocalls. https://www.ftc.gov/news-events/press-releases/2015/08/ftc-awards-25000-top-cash-prize-contest-winning-mobile-app-blocks. August. 17, 2015. (accessed January 22, 2017).

46 Ibid

47 Federal Trade Commission. Consumer Information: Prize Scams. http://www.consumer.ftc.gov/articles/0199-prize-scams (accessed January 18, 2017).

48 Federal Trade Commission. February 2016. *Consumer Sentinel Network Data Book for January-December 2015*. (February): 79 https:// www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2015/160229csn-2015databook.pdf (accessed on January 22, 2017).

49 Federal Trade Commission. February 2017. *Consumer Sentinel Network Data Book for January-December 2016*. (February): 79 https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2016/csn_cy-2016_data_book.pdf (accessed on January 30, 2018).

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

51 U.S. Congress. Senate. 2013. *876-SCAM: Jamaican Phone Fraud Targeting Seniors: Hearing before the Special Committee on Aging.* 113th Congress, 1st sess., March 13.

52 FairPoint Communications. FairPoint applauds Western Union decision to shut down services in Jamaican hotbed of phone scamming operations. BEWARE: Scams from Area Code 876. http://www.bewareof876.com/press-release-fairpoint-applauds-western-union-decision-to-shut-down-services-in-jamaican-hotbed-of (accessed January 22, 2017).

53 U.S. Senate, 876-SCAM, S. 6-7.

54 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. https://www.ice.gov/news/releases/jamaican-man-first-be-extradited-face-fraud-charges-lottery-scam (accessed January 22, 2017).

55 5 Federal Bureau of Investigation. Jamaican Man Sentenced to Prison for Involvement in International Lottery Fraud Scheme. https:// www.fbi.gov/minneapolis/press-releases/2015/jamaican-man-sentenced-to-prison-for-involvement-in-international-lottery-fraud-scheme (accessed

January 22, 2017).

56 Tillerson, Rex W. Remarks: Press Availability with Jamaican Prime Minister Andrew Holness. February 7, 2018. https://www.state.gov/secretary/remarks/2018/02/278085.htm (accessed on February 10, 2018).

57 Ibid.

58 Better Business Bureau. "BBB Warning: If Caller Asks "Can You Hear Me?," Just Hang Up. January 30, 2017. https://www.bbb.org/canyouhearme/ (accessed on September 29, 2017).

59 Barton, Genie. Prepared Statement of Genie Barton, President of the BBB Institute For Marketplace Trust Hearing on Robocall Scams. October 4, 2017. Pg. 11 https://www.aging.senate.gov/imo/media/doc/SCA_Barton_10_4_17.pdf (accessed on February 8, 2018).

60 Hernandez, Alesha. Calls Asking "Can you hear me now". FCC. March 21, 2017. https://www.consumer.ftc.gov/blog/2017/03/calls-asking-can-you-hear-me-now (accessed on September 22, 2017).

61 FTC Staff Briefing with Senate Aging Committee. September 5, 2017.

62 U.S. Congress. Senate. 2017. *Still Ringing off the Hook: An Update on Efforts to Combat Robocalls.* October 4, 2017. 48: 4-13.

63 Ibid.

64 FTC Staff Briefing with Senate Aging Committee. September 5, 2017.

65 Barton, Genie. Prepared Statement of Genie Barton, President of the BBB Institute For Marketplace Trust Hearing on Robocall Scams. October 4, 2017. Pg. 11

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

67 Federal Trade Commission. February 2016. *Consumer Sentinel Network Data Book, 82*. https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2016/csn_cy-2016_data_book.pdf (accessed on February 10, 2018)

68 Federal Trade Commission. February 2015. *Consumer Sentinel Network Data Book, 82*. https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2015/160229csn-2015databook.pdf (accessed on February 10, 2018)

69 Greisman, Lois. U.S. Congress. Senate. 2014. Hanging Up on Phone Scams: Progress and Potential Solutions to this Scourge: *Hearing before the Special Committee on Aging*. 113th Congress, 2nd sess., July 16. S.20

70 U.S. Congress. Senate. 2015. *Virtual Victims: When Computer Tech Support Becomes a Scam: Hearing before the Special Committee on Aging.* October 21. S. 22.

71 Ibid.

72 Federal Trade Commission. Staff Briefing. Dirksen Senate Office Building, G16. Washington, D.C. October 14, 2015.

73 Internet Crime Complaint Center. 2016 Internet Crime Report. 2017. Pg. 11-12 https://pdf.ic3.gov/2016_IC3Report.pdf (accessed on February 10, 2018).

74 Ibid.

75 U.S. Senate, Virtual Victims.

76 Ibid., S. 18.

77 Complaint at ¶ 19 FTC v. PCCare 247, Inc., et al., No 12-cv-7189 (S.D.N.Y.) (ECF No. 8).

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

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

80 Ibid.

81 Ibid.

82 Ibid.

83 Smith, Aaron and Monica Anderson. *5 Facts About Online Dating.* Per Research Center. Febraury 29, 2016. http://www.pewresearch.org/fact-tank/2016/02/29/5-facts-about-online-dating/ (accessed on February 16, 2018).

84 Ibid.

85 FBI, 2016 Computer Crime Report, 17. https://pdf.ic3.gov/2016_IC3Report.pdf (accessed on February 14, 2018).

86 Federal Trade Commission. Consumer Information:

Online Dating Scams. http://www.consumer.ftc.gov/articles/0004-online-datingscams (accessed January 22, 2017).

87 Federal Bureau of Investigation. Looking for Love? Beware of Online Dating Scams. https://www.fbi.gov/sandiego/press-releases/2013/looking-for-love-beware-of-online-dating-scams February 14, 2013. (accessed January 22, 2017).

88 FBI, 2016 Computer Crime Report, 18. https://pdf.ic3.gov/2016_IC3Report.pdf (accessed on February 14, 2018).

89 FBI. 2014 Computer Crime Report, 42. https://pdf.ic3.gov/2014_IC3Report.pdf (accessed on January 22, 2017).

90 Ibid.

91 U.S. Army Criminal Investigation Command Public Affairs. Army investigators warn public about romance scams. U.S. Army. http://www.army.mil/article/130861/Army_investigators_warn_public_about_romance_scams/. July 30, 2014. (accessed January 22, 2017).

92 Halpern, Mollie. "Podcast and Radio: Romance Scams." FBI This Week. https://www.fbi.gov/news/podcasts/thisweek/romance-scams.mp3/view. February 5, 2015. (accessed January 22, 2017).

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

94 National Center on Elder Abuse. Elder Abuse and Its Impact: What You Must Know. http://www.ncea.aoa.gov/Resources/Publication/ docs/NCEA_WhatYouMustKnow2013_508.pdf (accessed January 19, 2016)

95 Government Accountability Office. 2011. Elder Justice: Stronger Federal Leadership Could Enhance National Response to Elder Abuse. (March 21): 9.

96 Ibid., 14.

97 Ibid., 15

98 Elder Justice Initiative. Financial Exploitation FAQs. U.S. Department of Justice. http://www.justice.gov/elderjustice/financial/faq.html#do-all-states-have-elder-abuse-statutes-that-include-financial-exploitation (accessed January 18, 2016).

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

100 Ibid.

101 Ibid., 10

102 Culley, Denis and Jaye Martin. (2013). No Higher Calling—Representing Victims of Financial Exploitation. Bifocal 34, no. 5 (May-June): 89.

103 Department of Justice. Deputy Attorney General James M. Cole Speaks at the White House World Elder Abuse Awareness Day Event. http://www.justice.gov/opa/speech/deputy-attorney-general-james-m-cole-speaks-white-house-world-elder-abuse-awareness-day (accessed January 19, 2016).

104 Government Accountability Office. 2012. Elder Justice: National Strategy Needed to Effectively Combat Elder Exploitation. (November 15): 1.

105 The Patient Protection and Affordable Care Act, Subtitle H. Public Law 111-148. 111th Congress, 2nd sess.

106 GAO, Elder Justice, 22.

107 Ibid., 25-26

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

109 Financial Industry Regulatory Authority. FINRA Board Approves Rulemaking Item to Protect Seniors and Other Vulnerable Adults from Financial Exploitation. https://www.finra.org/newsroom/2015/finra-board-approves-rule-protecting-seniors-financial-exploitation (accessed January 21, 2016).

110 Metcalf, Andrew. 2015. Caretaker Sentenced for Stealing More than $400,000 from 87-Year-old Bethesda Man. Bethesda Magazine. October 10.

111 Ibid.

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

113 Ibid.

114 Ibid.

115 Ibid.

116 1 Russell, Eric. Maine Sunday Telegram. Victim of a Long Con Lives Out her Days Penniless in a Fryeburg Nursing Home. http:// www.pressherald.com/2016/11/27/victim-of-a-long-con-lives-out-her-days-penniless-in-a-fryeburg-nursing-home/ November 27, 2016. (accessed on January 22, 2017).

117 Ibid.

118 Ibid.

119 U.S. Government Accountability Office. (November 2016). Elder Abuse: The Extent of Abuse by Guardians Is Unknown, but Some Measures Exist to Help Protect Older Adults. (Publication No. GAO-17-33). Retrieved from GAO Reports Main Page via GPO Access database: http://gao.gov/assets/690/681088.pdf (accessed January 22, 2016).

120 Federal Trade Commission. 2016. Consumer Sentinel Network Data Book, 6. https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2016/csn_cy-2016_data_book.pdf (accessed on February 2, 2018).

121 Federal Trade Commission.2015 Consumer Sentinel Network Data Book, 6. https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-networkdata-book-january-december-2015/160229csn-2015databook.pdf (accessed on January 22, 2017).

122 Ibid., 14.

123 Marte, Jonnelle. 2015. You can now request copies of the phony tax returns filed in your name. *Washington Post*. November 10.

124 IRS. Key IRS Identity Theft Indicators Continue Dramatic Decline in 2017; Security Summit Marks 2017 Progress Against Identity Theft. February 8, 2018. https://www.irs.gov/newsroom/key-irs-identity-theft-indicators-continue-dramatic-decline-in-2017-security-summit-marks-2017-progress-against-identity-theft (accessed on February 10, 2018).

125 Ibid.

126 Medicare Access and CHIP Reauthorization Act of 2015. Public Law 114-10. 114th Congress, 2nd sess.

127 Centers for Medicare and Medicaid. Your Medicare Card. https://www.medicare.gov/forms-help-and-resources/your-medicare-card.html (accessed on February 8, 2018).

128 U.S. Congress. Senate. 2015. *Protecting Seniors from Identity Theft: Is the Federal Government Doing Enough?: Hearing before the Special Committee on Aging*. 114th Congress, 1st sess., October 7.

129 Ibid., S. 12-15 and S.17-20.

130 Hacket, Robert. *Equifax Underestimated by 2.5 Million the Number of Potential Breach Victims.* Fortune. October 2, 2017. http://fortune.com/2017/10/02/equifax-credit-breach-total/ (accessed on February 26, 2018).

131 Scam Alert: Con Artist Bank on Equifax breach. Better Business Bureau for Marketplace Trust. September 22, 2017. https://www.bbb.org/council/news-events/bbb-scam-alerts/2017/09/scam-alert-con-artists-bank-on-equifax-breach (accessed on September 27, 2017).

132 Better Business Bureau Scam Tracker. https://www.bbb.org/scamtracker/us

133 FTC. February 2015. 2015 Consumer Sentinel Network Data Book, 77 https://www.ftc.gov/system/files/documents/reports/consumersentinel-network-data-book-january-december-2015/160229csn-2015databook.pdf (accessed on January 22, 2017).

134 Ibid., 81.

135 Federal Trade Commission. February 2017. *Consumer Sentinel Network Data Book for January-December 2016*. (February): 81 https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2016/csn_cy-2016_data_book.pdf (accessed on January 30, 2018).

136 FTC. February 2015. 2015 Consumer Sentinel Network Data Book, 77 https://www.ftc.gov/system/files/documents/reports/consumersentinel-network-data-book-january-december-2015/160229csn-2015databook.pdf (accessed on January 22, 2017).

137 Frank. David. *Veterans Twice as Likely to Be Scammed.* AARP. November 8, 2017. https://www.aarp.org/money/scams-fraud/info-2017/veterans-scam-protection-fd.html (accessed on February 21, 2018).

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