114TH CONGRESS
2d Session

SENATE

REPORT
114–208

FIGHTING FRAUD: U.S. SENATE AGING COMMITTEE IDENTIFIES TOP 10 SCAMS TARGETING OUR NATION'S SENIORS

R E P O R T

OF THE

SPECIAL COMMITTEE ON AGING
UNITED STATES SENATE

February 11, 2016.—Ordered to the printed

U.S. GOVERNMENT PUBLISHING OFFICE
98–492 WASHINGTON : 2016

SENATE SPECIAL COMMITTEE ON AGING

SUSAN M. COLLINS, *Maine*
ORRIN HATCH, *Utah*
MARK KIRK, *Illinois*
JEFF FLAKE, *Arizona*
BOB CORKER, *Tennessee*
DEAN HELLER, *Nevada*
TIM SCOTT, *South Carolina*
TOM COTTON, *Arkansas*
DAVID PERDUE, *Georgia*
THOM TILLIS, *North Carolina*
BEN SASSE, *Nebraska*

CLAIRE MCCASKILL, *Missouri*
BILL NELSON, *Florida*
BOB CASEY, *Pennsylvania*
SHELDON WHITEHOUSE, *Rhode Island*
KIRSTEN GILLIBRAND, *New York*
RICHARD BLUMENTHAL, *Connecticut*
JOE DONNELLY, *Indiana*
ELIZABETH WARREN, *Massachusetts*
TIM KAINE, *Virginia*

PRISCILLA HOBSON HANLEY, *Majority Staff Director*
DERRON PARKS, *Minority Staff Director*

CONTENTS

LETTER OF SUBMITTAL

U.S. STATES SENATE,
SPECIAL COMMITTEE ON AGING,
Washington, DC, February 11, 2016.

Hon. JOE BIDEN,
President, U.S. Senate,
Washington, DC.

DEAR MR. PRESIDENT: Under authority of Senate Resolution 73 agreed to on February 12, 2015, I am submitting to you a report of the U.S. Senate Special Committee on Aging entitled: Stopping Senior Scams: The Top 10 Scams Reported to the U.S. Senate Special Committee on Aging's Fraud Hotline in 2015.

Senate Resolution 4, the Committee Systems Reorganization Amendments of 1977, authorizes the Special Committee on Aging "to conduct a continuing study of any and all matters pertaining to problems and opportunities of older people, including but not limited to, problems and opportunities of maintaining health, of assuring adequate income, of finding employment, of engaging in productive and rewarding activity, of securing proper housing and, when necessary, of obtaining care and assistance." Senate Resolution 4 also requires that the result of these studies and recommendations be reported to the Senate annually.

I am pleased to transmit this report to you.

Sincerely,

SUSAN M. COLLINS,
Chairman.

LETTER OF TRANSMITTAL

DEAR FRIENDS: Our nation's seniors worked hard their entire lives and saved for retirement. Unfortunately, there are many criminals who 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 people they trust. Many of these crimes are not reported because the victims are afraid that the perpetrator may retaliate, the victims are embarrassed that they have been scammed, or sometimes simply because victims 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 launched 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.

As the Chairman and Ranking Member of the Senate Special Committee on Aging, we remain 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 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.

Seniors are typically referred by investigators 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, con-

gressional caseworkers, or local nonprofits that provide assistance to seniors.

Over the past year the Fraud Hotline has been contacted by more than 1,100 individuals from all 50 states, the District of Columbia, and Puerto Rico. 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 who have worked with us to fight fraud.

In an effort to educate seniors on emerging trends and help protect them from becoming victims, this report features the top ten scams reported in 2015 to the Fraud Hotline. In addition, this report 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 2015 demonstrate the extent of this epidemic. In 2016, 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.*
CLAIRE MCCASKILL, *Ranking Member.*

114TH CONGRESS
2d Session

SENATE

REPORT
114–208

FIGHTING FRAUD: U.S. SENATE AGING COMMITTEE IDENTIFIES TOP 10 SCAMS TARGETING OUR NATION'S SENIORS

FEBRUARY 11, 2016.—Ordered to be printed

Ms. COLLINS, from the Special Committee on Aging, submitted the following

R E P O R T

EXECUTIVE SUMMARY

From January 1, 2015, through December 31, 2015, the Senate Aging Committee's Fraud Hotline received a total of 1,108 complaints from residents in all 50 states, the District of Columbia, and Puerto Rico. Calls pertaining to the top 10 scams featured in this report accounted for more than 90 percent of the complaints. The Committee has held hearings on the top seven scams on this list, with five of those hearings occurring in 2015.

The top complaint, the focus of more than twice as many calls as any other scam, involved seniors receiving 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, the Aging Committee held a hearing on April 15, 2015, to investigate and raise awareness about the IRS imposter scam.

Sweepstakes scams, such as the Jamaican lottery scam, continue to be a problem for seniors, placing second 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.

Nearly 100 seniors called to complain about receiving robocalls or unwanted phone calls, making that topic the third most common scam reported to the Committee. 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 cases.

Computer scams were fourth 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.

Identity theft was the fifth most common scam reported to the Fraud Hotline. 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 to assess the federal government's progress in complying with a new law to remove seniors' Social Security numbers from their Medicare cards, which will help prevent identity theft.

Grandparent scams, the focus of a July 16, 2014, 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 of money to cover an emergency, medical care, or a legal problem.

Elder financial abuse was seventh on the list and the topic of a February 4, 2015, hearing. The calls focused on the illegal or improper use of an older adult's funds, property, or assets. Chairman Susan Collins and Ranking Member Claire McCaskill introduced the Senior $afe Act of 2015, 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 eighth most common scam reported to the Fraud Hotline was grant scams. 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.

Romance scams were next 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 or months, 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 not occur.

Home improvement scams rounded out the top 10 scams reported to the Fraud Hotline in 2015. Seniors are common targets of these scams, in which fraudsters contact homeowners and offer to do home maintenance or yard work. The fraudsters charge the homeowners but either do not provide the service or do substandard work.

Key Figures

Rank	Type of Scam	Number of Complaints
1	IRS Impersonation Scams	387
2	Jamaican Lottery/Sweepstakes Scams	157
3	Robocalls/Unwanted Phone Calls	93
4	Computer Scams	87
5	Identity Theft	75
6	Grandparent Scams	63
7	Elder Financial Abuse	59
8	Government Grant Scams	37
9	Romance Scams	28
10	Home Improvement Scams	24

Figure 1. Top 10 Scams Reported to Aging Committee Fraud Hotline from January 1, 2015, to December 31, 2015 [1]

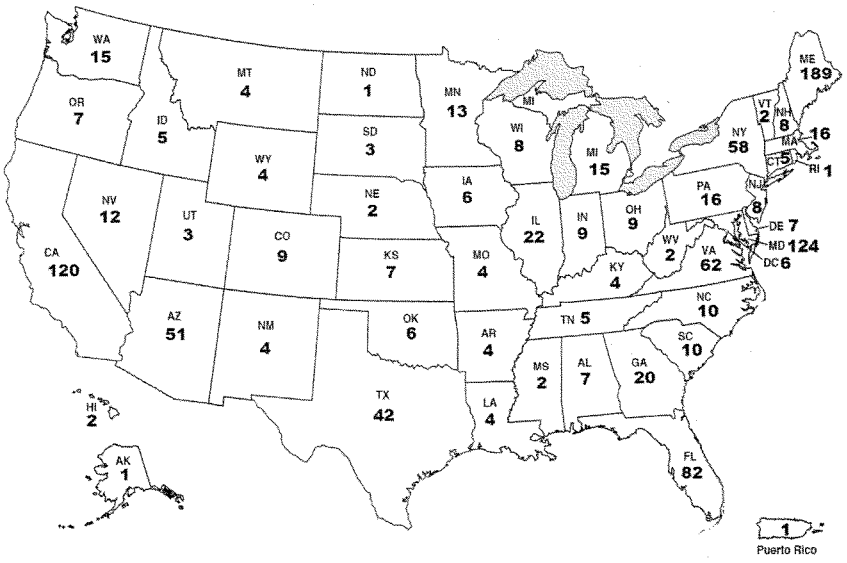

Figure 2. Origin of Calls Received by the Aging Committee's Fraud Hotline from January 1, 2015, to December 31, 2015[2]

[1] Please see Appendix 1 for a full list of scams reported to the Fraud Hotline in 2015

[2] Please see Appendix 1 for a table of the underlying data

TOP TEN SCAMS REPORTED TO THE SENATE AGING COMMITTEE'S FRAUD HOTLINE

1. IRS IMPERSONATION SCAMS

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, nearly 900,000 Americans have been targeted by scammers impersonating IRS officials, with 12,000 to 13,000 people submitting complaints on this scam every week as of December 2015.[2] Additionally, 30 to 50 people a week reported that they lost money to the scam; more than 5,000 Americans have lost a total of at least $26 million via this scam.[3] The IRS impersonation scam was the most frequent scam reported to the Fraud Hotline in 2015.

In response to the influx 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.[4] Since the hearing, the IRS has released several lists with tips to spot these scams and what people should do if they receive a call.[5]

TIGTA reports that increased awareness has made a difference, as it now takes scammers roughly 300 calls to find a victim as opposed to 50 calls prior to the Committee's hearing.[6] TIGTA reports, however, that the scam has morphed and evolved in response to guidance the IRS has issued.[7] 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.[8] 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, or pre-paid debit card. Victims are told that if they immediately pay the amount that is allegedly owed, the issue with the 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 indicated 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 remain hooked, the scammers will tell them they owe more money.

These scam calls most often involve a disguised, or "spoofed," caller identification (caller ID) number to make the victims believe that the call is coming from the "202" area code, the area code for Washington, D.C., where the U.S. Department of the Treasury and the IRS are headquartered. In a recent variation of this scam, calls also appear to be coming from the "509," "206," and "306" area

codes, all Washington State area codes. Scammers have also been known to "spoof" 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 are often willing to follow the supposed government official's instructions in order to resolve the alleged tax issue.

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.
Source: FCC

FRAUD CASE #1

"Lynn," from Ohio, called the Fraud Hotline after she learned that her mother had been scammed out of $1,600. Lynn said that her mother received a phone call from a scammer posing as an IRS agent. The scammer recited a number he claimed was on his IRS badge and tricked Lynn's mother into believing that he was an authentic IRS agent. The alleged IRS agent told her mother that they had a warrant for her arrest for failing to pay her taxes from 2012, and unless she paid them today, they were going to send the police to her house and arrest her. The scammer directed her to go to her local grocery store and buy a prepaid debit card. After obtaining the debit card and loading it with $500, she read the scammer the 16-digit PIN number on the back of the card, which allowed the scammer to steal the card's funds. Upon doing so, the scammer told her that, after a closer look at her records, it appeared that she owed additional taxes for previous years. The scammer directed her to buy another prepaid debit card and took the money from that card as well. The scam continued until Lynn visited her mother and learned what was happening. A Fraud Hotline investigator filed a report with TIGTA on Lynn's behalf. In addition, the investigator gave Lynn and her mother tips to avoid being scammed again.

As of December 31, 2015, the Department of Justice had only prosecuted three individuals for their roles in the IRS impersonation scams. Two of these individuals were prosecuted in Florida, and the other individual was prosecuted in New York. In July 2015, the New York perpetrator was sentenced to more than 14 years in prison and ordered to forfeit $1 million for crimes that stretched from December 2011 until his December 2013 arrest.[9]

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.

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

FRAUD CASE #2

"Mrs. A," from Maine, was scammed out of $23,000 after receiving a call from someone claiming to be from the IRS. Mrs. A was instructed to send wire-transfers

and purchase money orders, as well as make deposits in specific bank accounts. When the phone call was accidentally disconnected, Mrs. A received a call from a "Lt. Green" from a number that displayed on her caller ID as her local police department. The con artist said that she should not hang up on the IRS and told her that, should she hang up again, he would arrest her. This led her to believe that the previous call was in fact from the IRS. In addition, she also received a call that displayed as the local district attorney's office. After eventually becoming suspicious that something was amiss, she went to her local police department, which began investigating the calls. As Mrs. A was being interviewed by a detective, the imposter once again called the victim's cell phone. The detective took the call and did not let the scammer speak to Mrs. A. The detective spoke to her bank's fraud department and was able to stop a pending wire transfer to an account overseas. As a result, Mrs. A received $11,000 of her money back. A Fraud Hotline investigator spoke with both the victim and the local detective in the case. The local detective testified at the Committee's hearing in April 2015. TIGTA took over this case.

2. SWEEPSTAKES SCAMS

Sweepstakes scams continue to claim senior victims who believe they have won a lottery and only need to take a few actions to obtain their winnings. Scammers will 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.[10] According to the Federal Trade Commission (FTC) the number of sweepstakes scams increased by 5.68 percent between 2013 and 2014.[11]

Early last Congress, the Aging Committee launched an investigation of the Jamaican lottery scam, one of the most pervasive sweepstakes scams.[12] 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.[13]

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.[14] Several arrests have been made 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."[15]

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 the victims that they have won the Jamaican lottery or a brand new car and that they must wire a few hundred dollars for upfront processing fees or taxes for their winnings to be delivered. Often, the criminals will 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 cards, electronic wire transfers, money orders, and even cash.

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.[16] Criminals once involved in narcotics trafficking have found these scams to be safer and more lucrative.

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

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.

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 (FBI), the Social Security Administration, and the Department of Homeland Security (DHS), asking for personal data and bank account numbers so that they can "solve" the crime.

FRAUD CASE #3

"Carol," from Washington State, called the Fraud Hotline regarding her father, who had been the victim of the Jamaican lottery scam. Over the past five and a half years, Carol's father lost more than $600,000. Her father is a former Navy Captain and Korean and Vietnam War veteran.

Carol used to give her parents $500 twice a month for expenses. Sometimes she would send more because her mother would call saying that her father had given away all of their money to con artists associated with the Jamaican lottery scam. In July, Carol began sending her parents food and gas cards and paying all of their bills directly in lieu of sending cash. When her parents stopped receiving cash, the lottery scammers acquired her father's personal information, contacted the Defense Financial and Accounting Administration, and rerouted his pension to one of their accounts. The scammers apparently "spoofed" the call to make it appear as though they were calling from the same area code in which Carol's parents live.

A Fraud Hotline investigator helped Carol contact the DHS and the local FBI field office in California. The investigator also helped Carol provide both agencies with copies of her father's recent Verizon bill showing the numerous calls from the 876 area code, the country code for Jamaica, along with the corresponding dates and times. The DHS and the FBI both said that this case was one of the largest they had ever seen. The Fraud Hotline investigator was able to have the July pension check reissued to Carol's father and helped arrange to have future pension payments deposited in a family trust where scammers would not have access to the funds.

3. ROBOCALLS/UNWANTED 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.[17] Unfortunately, 12 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. Robodialers can be used to distribute pre-recorded messages or to connect the person who answers the call with a live person.

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

Robocalls often originate offshore. 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 previous section on Internal Revenue Service (IRS) impersonation scams, fraudsters spoof their numbers to make victims believe they are calling from the government or another legitimate entity. In addition, scammers will often spoof numbers to appear as if they are calling from the victims' home states or local area codes.

Robocalls have become an increasing nuisance to consumers in recent years due to advances in technology. Phone calls used to be routed through equipment that was costly and 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 practically 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 can reach.

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.

Many companies now offer third-party spoofing and robodialing services. Third-party spoofing companies provide an easy-to-use computer interface or cell phone app that allows calls to be spoofed at a negligible cost. To demonstrate how accessible this technology is, an Aging Committee staff member spoofed two separate calls to Chairman Susan Collins during a Committee hearing on June 10, 2015, titled "Ringing Off the Hook: Examining the Proliferation of Unwanted Calls."[18] By using an inexpensive smartphone app, the staff member was able to make it appear that the calls were from the IRS and the Department of Justice, respectively. 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 advances in telephone technology makes it easier for scammers to cast a wide net and increase the number of potential victims they can reach, and highlighted possible technological solutions to this menace.[19]

FRAUD CASE #4

Linda Blase, from Texas, testified at the Aging Committee's June 2015 hearing that she had been plagued by robocalls for years. She described how these calls had disrupted her personal life and the small business she operated out of her home. Although Linda had registered with both the national Do-Not-Call registry and her state's registry, she continued to receive telemarketing calls and an increasing number of government impersonation scam calls. Linda began keeping a log of these calls and also began using a call blocking device to limit the number of nuisance calls to her home. Like many other seniors, Linda did not feel comfortable letting the phone ring or screening calls since she did not want to miss an important medical or business-related call. This led her to bring this problem to the attention of the Committee in the hope that a solution could be found.

In response to the high volume of robocalls that are made in violation of the national Do-Not-Call registry, the Federal Trade Commission (FTC) launched a contest in October 2012 to identify inno-

vative solutions to protect consumers from these calls.[20] In April 2013, the FTC announced that Nomorobo, a free service that screens and blocks robocalls made to VoIP phone numbers, was one of two winners of the their Robocall Challenge.[21]

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.[22] If the caller is on the whitelist, the phone continues to ring, but if the number is on the blacklist, the call will disconnect after one ring. Aging Committee Fraud Hotline investigators have referred callers who contact the Hotline regarding robocalls to the Nomorobo website and have received positive 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 crowd-sourced "honeypot" and to better analyze data from an existing honeypot.[23] In this context, a honeypot is an information system that attracts robocalls so that researchers can analyze them and develop preventive techniques.[24] In August 2015, the FTC announced that RoboKiller, a mobile app that blocks and forwards robocalls to a crowd-sourced honeypot, was selected as the winner of the Robocalls: Humanity Strikes Back contest.[25] 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.[26]

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

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

Source: *https://consumercomplaints.fcc.gov/hc/en-us/articles/202654304–Spoofing-and-Caller-ID*

4. COMPUTER SCAMS

The Aging Committee saw an increase in the frequency and severity of computer-based scams in 2015. Private industry has 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.[27] The company estimated that 3.3 million Americans are victims of technical support scams annually, with losses of roughly $1.5 billion per year.[28] 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.[29] In addition, in 2014, the Internet Crime Complaint Center (IC3),

a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center, received 269,492 computer fraud complaints with a loss of $800,492,073.[30] Americans age 60 and older accounted for 16.57 percent of these complaints.[31]

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."[32] The hearing featured representatives from Microsoft and the Federal Trade Commission (FTC) who spoke about the challenges in combating this fraud given its many variations and constant changes.[33]

FRAUD CASE #5

Frank Schiller, from Maine, testified at the Aging Committee's hearing on computer tech support scams in October 2015. 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 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 surfing the Internet may see a pop-up window on their computer instructing them to contact a tech-support agent. Sometimes, scammers have used the pop-up window to hack into victims' computers, lock them out, and require victims to pay a ransom to regain control of their computers. Below are several of the most common variations of this scam:

- Scammers Contact Victims. In the most prevalent variation of this scam, con artists randomly call potential victims and offer to clean their computers and/or sell them a long-term or technical support "service." The con artists usually direct victims' computers to display benign error messages that appear on every computer to convince victims that their computers are malfunctioning. Scammers generally charge victims between $150 and $800 and may install free programs or trial versions of antivirus programs to give the illusion that they are repairing victims' computers. If victims express concern about the price, the con artists will often entice victims to pay by offering a "senior citizen discount."
- 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 "spon-

sored 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.[34] Some key search terms included: "virus removal," "how to get rid of a computer virus," "McAfee Customer Support," and "Norton Support." These search terms are cleverly chosen to confuse the consumer into thinking the fraudsters are associated with well-known companies. Other fraudsters use pop-up messages on consumers' computer screens that direct potential victims to call them.

- Ransomware. Scammers use malware or spyware to infect victims' computers with a virus or encrypt the computers so they cannot be used until a fee is paid. If victims refuse to pay, scammers will render the computer useless, prompting the appearance of a blue screen that can only be removed with a password known by the scammers. The Fraud Hotline has received reports that scammers sometimes admit to victims that it is a scam and refuse to unlock the victims' computers unless a "ransom" payment is made.
- Fraudulent Refund. Scammers contact victims stating 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 the consumers.

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.[35]

FRAUD CASE #6

"Karl," from Florida, called the Aging Committee's Fraud Hotline after he realized that he had been the victim of a computer scam. Karl said he had received a call from someone claiming to be from Microsoft. The scammer told Karl that his computer had been hacked and was about to crash. The "technician" instructed Karl to go to his computer and click on programs so he could show him the problem. When Karl did so, the scammer was able to access his computer, and an error message subsequently appeared on the screen. Karl was told that his computer could be cleaned for $300. Karl agreed and gave the con artist his credit card number. The next day, Karl received another call from an individual claiming to be from Microsoft, who told him that his computer needed to be updated again. This time, it was going to cost $150. At this point, Karl realized that he had been scammed. Karl called an Aging Committee Fraud Hotline investigator, who told him that these scams were prevalent and recommended ways he might protect himself in the future. Karl was encouraged to contact his credit card company, the IC3, and his local police department. He was also encouraged to have his computer cleaned by a local computer repair service to ensure that the scammers did not download malware.

Tips from the 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 pop-up blockers.

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

5. IDENTITY THEFT

Identity theft has been the Federal Trade Commission's (FTC) most common consumer complaint for the past 15 years, with 212,698 Americans reporting being victimized in 2014 alone.[36] Nearly 40 percent of the identity theft complaints that the FTC received in 2014 were reported by consumers age 50 and older.[37]

Identity thieves not only disrupt the lives of individuals by draining bank accounts, making unauthorized credit card charges, and damaging credit reports, but they also often defraud the government and taxpayers by using stolen personal information to submit fraudulent billings to Medicare or Medicaid or apply for and receive Social Security benefits to which they are not entitled. Fraudsters also use stolen personal information, including Social Security numbers (SSN), to commit tax fraud or to fraudulently apply for jobs and earn wages. According to the FTC, government documents/benefits fraud was the most common type of identity theft reported by consumers in 2014, comprising 38.7 percent of all identity theft complaints.[38]

FRAUD CASE #8

"Amanda," from Maine, contacted the Fraud Hotline after she learned that she had been the victim of identity theft. When Amanda tried to file her taxes online electronically, she was notified that someone had already submitted a tax return using her and her husband's names and SSNs. She was told that it could take between three and six months for the issue to be resolved and for her to receive her tax return. A Fraud Hotline investigator was able to work with Amanda and her local Taxpayer Advocate Service to process her return in five weeks. Once Amanda received her refund, the Taxpayer Advocate advised her that the Internal Revenue Service would apply extra scrutiny to her return for the next three years to help ensure that no one tries to use her name and SSN to submit another fraudulent return.

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

Tax-related identity theft continues to disrupt the lives of Americans. The growing use of commercial tax filing software and online tax filing services has led to opportunities for thieves to commit fraud without stealing SSNs. In some cases, thieves can illegally access an existing customer's account simply by entering that indi-

vidual'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 he files 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 longstanding policy and now will provide victims with copies of the fake returns upon written request.[39] The documents will provide victims with details to help them discover how much of their personal information was stolen.

Medical identity theft occurs when someone steals personal information—an individual's name, SSN, or health insurance claim number (HICN)—to obtain medical care, buy prescription drugs, or submit fake billings to Medicare. Medical identity theft can disrupt lives, damage credit ratings, and waste taxpayer dollars. Some identity thieves 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.

FRAUD CASE #7

"Katie," from Maine, contacted the Fraud Hotline after she received a credit card bill in the mail from Victoria's Secret in the amount of $730.45. Katie, who is in her 70s, said that she is certain that she never purchased anything from Victoria's Secret. The bill indicated that someone opened a Victoria's Secret credit card at a Florida location in August. The statement showed two transactions: the first one in the amount of $30 for lip-gloss, and the second transaction totaling $700 in gift cards. Most likely, whoever opened the card ran the first charge as a test to make sure it would work. Katie had already filed a police report with her police department and contacted Victoria's Secret. Victoria's Secret cancelled the card and is not holding Katie responsible for the charges. A Fraud Hotline investigator explained to Katie that she should notify one of the three national credit reporting companies to place a fraud alert on her credit report. By placing a fraud alert, she is also entitled to a free copy of her credit report to see if there has been any other fraudulent activity committed under her name or SSN. The investigator also filed a report with the FTC on Katie's behalf.

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.[40] On October 7, 2015, the Aging Committee held a hearing titled, "Protecting Seniors from Identity Theft: Is the Federal Government Doing Enough?"[41] The Committee heard testimony from the CMS official in charge of implementing the Medicare card replacement process and from the Health and Human Services Office of Inspector General about investigative efforts to combat medical identity theft.[42]

What To Do if You Suspect You Are a Victim of Identity Theft

What To Do Right Away:

1. Call the companies where you know the fraud occurred.

2. Place a fraud alert with a credit reporting agency and get your credit report from one of the three national credit bureaus.
3. Report identity theft to the 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 alert or credit freeze.

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

6. 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 victim's 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 the money is wired, it is difficult to trace.

The Fraud Hotline has received frequent reports of con artists telling victims that they were 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 electronic 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. Often, scammers 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.

FRAUD CASE #9

"Katelyn," from Maryland, contacted the Fraud Hotline to report that her mother had been the victim of a grandparent scam. Katelyn said that when her mother, "Meredith," answered the phone, a young man said, "Hi Grammy, I've had an accident in the Bahamas and need help." Meredith thought it was her grandson Kyle and asked what she could do to help. The con artist told her that he needed $9,000 to pay for towing and hospital fees, as well as money to help get back home since the car had been totaled. He begged her not to tell his mom. Meredith was instructed to drive to the local Western Union location and wire the money, which she quickly did. When Meredith returned home, the con artist called her again and asked for more money. Meredith became suspicious and called her daughter, who told her that Kyle was not in the Bahamas and was home earlier that day. Her county sheriff's department referred Katelyn to the Fraud Hotline, where an investigator helped her file a report with Western Union's Fraud Department, the FTC, and the DHS.

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 artists impersonating victims' grandchildren to talk briefly with the victims and then hand the phone over to an accomplice impersonating an

authority figure. This gives the scammers' stories more credibility and reduces the chance that the victims will recognize that the voice on the phone does not belong to their grandchild.

In 2014, the FTC received 14,521 complaints of individuals impersonating friends and family members, up from 11,793 in 2012.[43] 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.[44]

FRAUD CASE #10

"Jackie," from Kentucky, called the Fraud Hotline to report that she had been the victim of a grandparent scam. Jackie told investigators that she had answered a phone call and heard a young man's voice on the phone respond, "Grandma." Jackie asked if it was "Tommy," her grandson. The man responded, "Yes, this is Tommy." Jackie told a Fraud Hotline investigator that "her grandson" on the phone said he was in Orlando with some friends when the police pulled their car over and arrested them for drug possession. The con artist told her that he was not using any drugs and did not know they were in the car. He told Jackie he needed money to post bail so he could come home. That is when the phone was handed to another individual who was allegedly a bondsman. The bondsman instructed Jackie to go to her local Walmart and buy $4,000 in iTunes gift cards. The bondsman told her she needed to do it quickly, because if she did not have all the cards within an hour when he called back, the bail was going to increase to $6,000. Once Jackie purchased the cards, she read the numbers on the back of the cards to the scammers. She was then told that there were additional fines and that she would need to send an additional $1,500. At this point, Jackie realized she had been scammed. Jackie called her grandson, who was safe at home. Jackie explained to the Fraud Hotline investigator that she wished she had asked a question that only her true grandson could have answered. By the time Jackie called the Fraud Hotline, she and her grandson had already filed a complaint with Apple's Fraud Department and the local police department. The Fraud Hotline investigator filed a report with the Federal Trade Commission (FTC) and the Department of Homeland Security (DHS) on Jackie's behalf. The investigator also gave Jackie tips on how to avoid being scammed over the phone in the future.

7. 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.[45] One study found that, for every case of financial fraud that is reported, as many as 14 go unreported.[46] 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.[47]

The Fraud Hotline documents complaints of elder abuse and refers callers to Adult Protective Services (APS) for further action. APS employees receive reports of alleged abuse, investigate these allegations, determine whether or not the alleged abuse can be substantiated, and arrange for services to ensure victims' well-being.[48] APS can also refer cases to law enforcement agencies or district attorneys for criminal investigation and prosecution.[49] 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.[50]

FRAUD CASE #11

"Richard," from Arizona, called to report that his 84-year-old father, who has Alzheimer's, was the victim of financial elder abuse. Richard said that six months after his mother died, a 33-year-old woman started interacting and caring for his father. Richard claimed that she and her family depleted his father's accounts and convinced him to sell his house. The woman is preventing Richard and other family members from seeing his father. A Fraud Hotline investigator spoke with Richard and provided him with the number for his state's APS and attorney general's office.

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.[51] Most victims are between the ages of 80 and 89, live alone, and require support with daily activities.[52] 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.[53]

Victims whose assets have been taken by family members typically do not want their relatives to be criminally prosecuted, leaving civil action as the only mechanism to recover stolen assets.[54] Few civil attorneys, however, are trained in issues related to older victims and financial exploitation.[55] 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.[56]

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.[57] The law formed the Elder Justice Coordinating Council, which first convened on October 11, 2012, and is tasked with increasing cooperation among federal agencies.[58] 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.[59]

While some states have laws that require financial professionals to report suspected financial exploitation of seniors to the appropriate local or state authorities, there currently is no federal requirement to do so. Some financial professionals may fail to report suspected financial exploitation due to a lack of training or fear of repercussions for violating privacy laws. In October 2015, Aging Committee Chairman Susan Collins and Ranking Member Claire McCaskill introduced the *Senior$afe Act of 2015*, which would provide certain individuals with immunity for disclosing suspected financial exploitation of senior citizens.[60] The Financial Industry Regulatory Authority is simultaneously pursuing rulemaking that would empower financial professionals to protect their senior clients from financial abuse.[61] In the private sector, Wells Fargo has established internal training programs for its employees so that they are better equipped to detect and prevent financial abuse before it occurs.[62]

FRAUD CASE #12

"Mackenzie," from Arizona, contacted the Fraud Hotline when she noticed that her daughter, who holds power of attorney, had been taking money out of her account without her permission. Mackenzie told a Fraud Hotline investigator that she is coherent and does not suffer from any diminished capacity. The investigator pro-

vided Mackenzie with the number for her state's APS and her local Area Agency on Aging to help her resolve the matter.

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, embezzled more than $400,000 before one of the victim's bankers discovered suspicious activity in his account and alerted APS.[63] The fraudster had convinced the victim to give her power of attorney and control over his finances. She was sentenced to five years in jail for financial exploitation of a vulnerable adult, theft, and embezzlement.[64]

The Aging Committee has brought to light many schemes that have defrauded seniors out of their hard-earned retirement savings. It is deeply troubling when a senior falls victim to one of these schemes, but it is even more egregious when the perpetrator is a family member, caregiver, or trusted financial adviser. At the Aging Committee's first hearing of the 114th Congress, "Broken Trust: Combating Financial Exploitation of Vulnerable Seniors," Philip Marshall, the grandson of well-known philanthropist Brooke Astor, testified that his father, Anthony Marshall, mistreated his mother and mismanaged her assets while she suffered from Alzheimer's disease.[65] In 2009, after a six-month criminal trial, Mr. Marshall's father was found guilty on 13 of the 14 counts against him.[66]

8. GRANT SCAMS

Grant scams, of which there are multiple variations, are frequently reported to the Aging Committee's Fraud Hotline. In the most common version of this scam, consumers receive an unsolicited phone call from con artists claiming that they are from the "Federal Grants 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." Scammers 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, "[d]eceptive 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."[67] According to FTC data, the frequency of Americans reporting grant scams has dropped over the past three years.[68] In 2014, the FTC received 8,032 complaints, which was about a 10 percent decrease from the prior year.[69]

FRAUD CASE #13

"Carol," from West Virginia, called the Fraud Hotline to report a voicemail she received from someone claiming to be from the "U.S. Government Grant Office." Although the phone number did not display on her caller ID, the voicemail directed her to call a 202 number, which is the area code for Washington, D.C. When she called the number, the man who answered told her that she had been awarded a $7,000 grant, but she had to pay $475 in taxes to receive it. Carol knew this was a scam and hung up immediately. Although Carol did not lose any money, a Fraud Hotline investigator filed a complaint with the FTC, Treasury Inspector General for

Tax Administration (TIGTA), and the Department of Homeland Security (DHS) on her behalf.

FRAUD CASE #14

"Charles," from Maine, contacted the Aging Committee's Fraud Hotline to report a call he received from someone claiming to be from the "Federal Grant Administration" congratulating him on receiving a government grant in the amount of $9,000. The number contained a 202 area code, which belongs to Washington, D.C. The scammer told Charles that he had to pay a fee of $280 and gave him a number for him to call the "Federal Bank" to get details on how to receive his grant. The number for the "Federal Bank" had a 646 area code, which belongs to New York City. When Charles called the "Federal Bank," someone answered "Federal Bank," took his name, and explained to him that, in order to receive his grant, he had to send them a Western Union wire transfer. Charles went to his local Western Union outlet and sent the wire transfer. When Charles called the bank back to see if it had received the transfer, he was told that there was another fee that the bank was not initially aware of. That is when he realized he had been scammed. A Fraud Hotline investigator helped Charles file a complaint with TIGTA, the FTC, the Western Union fraud department, and the DHS. The investigator also contacted the local Western Union location to alert them to the fraud. The investigator explained that these scam calls are often geographically based and that it is likely that others in the area may receive these calls.

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*

9. ROMANCE SCAMS/CONFIDENCE FRAUD

More and more Americans are turning to the Internet for dating. As of December 2013, one in 10 American adults had used online dating services, and online dating is now a $2 billion industry.[70] 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. Sometimes these reports were not just from seniors, but also from friends and family members whose loved ones were deeply involved in a fictitious cyber-relationship. This is one of the most heartbreaking scams because con artists exploit seniors' loneliness and vulnerability.

In a related scam known as confidence fraud, con artists gain the trust of 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 rank and name 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 artists 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), 12 percent of the complaints submitted in 2014 contained a social media aspect.[71] Con artists have been known to create elaborate profile pages, giving their fabricated story more credibility. Con artists often call and chat on the phone to prove that they are real. These conversations can take place over weeks and even months as the con artists build trust with their victims. In some instances, con artists have even promised to marry their victims.

2014 FBI COMPLAINTS OF CONFIDENCE FRAUD AND ROMANCE SCAMS

Age Range	Complaints	Loss
Under 20	30	$37,432
20–29	457	$614,295
30–39	929	$3,765,553
40–49	1,575	$21,285,533
50–59	1,805	$34,659,425
Over 60	1,087	$26,350,745
Total	5,883	$86,713,003

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

Inevitably, con artists in these scams will ask their victims for money for a variety of things. Often the 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 bills, hospital bills for a child or other relative, visas or other official documents, or losses from a temporary financial setback.[72] Unfortunately, in spite of telling their victims they will never ask for any more money, something always comes up resulting in the con artists 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.[73]

In 2014, the FBI's IC3 received more than 5,883 complaints about romance and confidence scams that cost victims $86.7 million dollars.[74] Nearly half of these victims were age 50 or older, and this group accounted for approximately 70 percent of the money lost to this scam last year.[75] Romance and confidence scams disproportionally target women, usually between the ages of 30 and 55 years old.[76] Unfortunately, both the amount of financial loss and the number of complaints for this crime have increased in recent years.[77]

FRAUD CASE #15

"Debbie," from Maine, contacted the Fraud Hotline to report that she had lost more than $140,000 in an online dating scam. The scam began in May 2014 when she met a man on the website "plentyoffish.com," who claimed to live in Miami. The man, who said his name was "Lex," told Debbie that his employer was sending him

to Benin in Africa. The pair continued to correspond, and, two months later, Lex told Debbie that his bank accounts were frozen and he needed her to send him money until he could regain access to his accounts. She started wiring money from MoneyGram and pre-paid debit cards in $2,000 to $3,000 increments to an address in Benin. After a while, Debbie became suspicious that this was a scam and stopped sending money. Then, in October 2014, she received emails from a bank she believed was real, saying it could reimburse her for the money she sent to Lex. The emails were fake, possibly from the same scammer, and charged her thousands of dollars in processing fees. She ended up transferring $40,000 into different bank accounts in the United States. In all, Debbie lost more than $140,000 to this scam. Debbie provided a Fraud Hotline investigator with more than 400 pages of emails and wire transfer receipts. The investigator reported the crime to the FTC, the FBI's IC3, and the Department of Homeland Security.

Tips From The FBI's IC3 To Help Prevent Victims 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*

10. HOME IMPROVEMENT SCAMS

The last of the top 10 scams reported to the Fraud Hotline in 2015 were home improvement scams. There are several variations of this scam in which scammers show up at victims' doors and offer to perform a service for a price that seems fair. These service jobs frequently involve, but are not limited to, repairing a roof, repaving a driveway, repainting a house or room, or installing a home security system. The contractors usually ask for immediate payment in advance but then do substandard work, or no work at all. Seniors, those who live alone, individuals with disabilities, and victims of weather-related disasters are common targets.[78]

Home improvement scams occur frequently during a change of season. Con artists will often take advantage of the warmer weather, or approaching cooler weather, and use it as an opportunity to convince victims that it is the perfect time to get home improvement jobs done. In 2014, the Federal Trade Commission (FTC) received 8,327 complaints about home repair, improvement, and product scams.[79]

2014 FEDERAL BUREAU OF INVESTIGATION'S COMPLAINTS OF HOME IMPROVEMENT SCAMS

Home Appliances	1,681
Home Furnishings	1,001
Home Protection Devices	823
Home Repair	1,856
Housing	2,997
Total:	8,327

Source: *https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2014/sentinel-cy2014-1.pdf.*

FRAUD CASE #16

"Samson," from Texas, contacted the Fraud Hotline to report that he had paid a contractor $10,000 to repair one side of his roof. After the work was completed, how-

ever, his roof started to leak again. Samson said that he had been trying for more than a month to get in contact with the contractor, but to no avail. Samson heard about the contractor through an advertisement in the local newspaper. A Fraud Hotline investigator encouraged Samson to contact the Texas Attorney General's Office of Consumer Protection, the Texas Commission of Licensing and Regulation, and the Texas Legal Services Center.

Scammers will also frequently target individuals who have been affected by a recent weather-related disaster. Con artists may appear after a storm, promising to help with immediate clean-up and debris removal. For instance, after a flood, these scammers may tell victims that they can restore their appliances or haul away damaged items for a fee. Scammers then demand immediate payment for work that they will never do.[80] Unlicensed and unskilled contractors may also offer to restore damaged homes and then fail to do the work or do a substandard job. Since flooding can cause lasting problems, such as mold, it's important that homeowners verify that any company they are considering to clean or repair their homes has the proper licenses, insurance, and experience to do the job.

FRAUD CASE #17

"Hannah," from Mississippi, contacted the Fraud Hotline to report that she had been scammed out of $3,000. Hannah was approached by a contractor who noticed that her driveway was cracked and had several potholes and bumps. The contractor indicated that he had just finished a job in the neighborhood and that he could give her a good deal on repairing her driveway. Hannah agreed and gave the contractor a $1,500 deposit. The contractor, however, never returned to do the job. Hannah had not signed a contract, nor did she have the contractor's phone number. Hannah was encouraged to contact Mississippi's Attorney General's Office of Consumer Protection and her local police department.

Another example of the home improvement scam involves home security systems. Scammers may show up at victims' doors, inform them about a string of robberies in the area, and offer to sell them a home alarm. The device they install may or may not be a working device, or the victims may unknowingly pay more than market price. In a new variation of this scam, con artists knock on victims' doors and claim that they are there to upgrade the home security system. In November 2015, the FTC warned that scammers may purport to work for a home security company the victim already uses, but instead install a new system without asking and convince the victim to sign a new contract.[81] Most people do not know that they have been scammed until their original home security company notifies them that their system is not responding, or they start receiving bills from two different alarm companies.[82]

FTC's Tips on How Tell if a Contractor Might Not Be Reputable

Don't do business with someone who:

- Claims that "the deal is good for today only." Often, con artists will pressure you for an immediate decision by telling you that, if you wait even another day, they cannot guarantee the same price.
- Lacks professionalism. Ask if the person has a business card, or check to see if the person's vehicle is marked with a company logo or information.
- Only accepts cash; asks you to pay everything, or a sizeable deposit, upfront; or tells you to borrow money from a lender the contractor knows.

• Is not licensed. Many states, but not all, require contractors to be licensed and/or bonded. Check with your local building department or consumer protection agency to learn about licensing requirements in your area.

• States that he "just happens to have materials left over from a previous job" or "just happens to be in the area."

Source: *https://www.consumer.ftc.gov/blog/home-improvement-scams-are-no-laughing-matter*

CONCLUSION

One of the Senate Special Committee on Aging's top priorities in the 114th Congress has been to combat fraud targeting seniors. The Fraud Hotline has been instrumental in this fight, providing more than 1,100 callers in 2015 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 held hearings on five of the top 10 scams reported to the Fraud Hotline in 2015. The Committee's hearings have helped to 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. Chairman Susan Collins and Ranking Member Claire McCaskill have pressed federal law enforcement agencies to combat fraud and put the criminals who prey on our nation's 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. As the Aging Committee enters its second year of the 114th Congress, Chairman Collins and Ranking Member McCaskill intend to maintain the Committee's focus on frauds targeting seniors. In order to encourage a more effective federal response to these scams, the Chairman and Ranking Member will continue to work with their Senate colleagues to ensure that law enforcement has the tools it needs to pursue these criminals.

This report 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, please do not hesitate to call the Fraud Hotline at 1–855–303–9470.

Appendix 1: Aging Fraud Hotline Statistics

Scam Type	Total
IRS Impersonation Scams	387
Jamaican Lottery/Sweepstakes Scams	157
Unsolicited/Unwanted Phone Calls	93
Computer Scams	87
Identity Theft	75
Grandparent Scams	63
Elder Financial Abuse	59
Government Grant Scams	37
Romance Scams	28
Home Improvement Scams	24

Scam Type	Total
Bad Business Practices	23
Spam Emails	18
Junk Mail	7
Check Scam	6
IRS Fraudulent Tax Returns	5
Utility Scam	5
Health Care Scam	4
Counterfeit Scam	3
Medical Equipment	3
Mortgage Fraud	3
Phishing Phone Call	3
Nigerian Prince Inheritance Scam	3
Debt Collection Scam	3
Investment Scam	2
Nigerian Gold Scam	2
Bad Landlord	1
Disability Enrollment Scam	1
International Drug Trafficking Scam	1
Life Insurance Scam	1
Military Impersonation Scam	1
Online Military Impersonation Scam	1
Payday Loan Scam	1
SSDI Issues	1
Total	1108

Origin of Calls to the Hotline	Total	Origin of Calls to the Hotline	Total
Alabama	7	Nebraska	2
Alaska	1	Nevada	12
Arizona	51	New Hampshire	8
Arkansas	4	New Jersey	8
California	120	New Mexico	4
Colorado	9	New York	58
Connecticut	5	North Carolina	10
Delaware	7	North Dakota	1
District of Columbia	6	Ohio	9
Florida	82	Oklahoma	6
Georgia	20	Oregon	7
Hawaii	2	Pennsylvania	16
Idaho	5	Puerto Rico	1
Illinois	22	Rhode Island	1
Indiana	9	South Carolina	10
Iowa	6	South Dakota	3
Kansas	7	Tennessee	5
Kentucky	4	Texas	42
Louisiana	4	Unknown	71
Maine	189	Utah	3
Maryland	124	Vermont	2
Massachusetts	16	Virginia	62
Michigan	15	Washington	15
Minnesota	13	West Virginia	2
Mississippi	2	Wisconsin	8
Missouri	4	Wyoming	4
Montana	4		

Appendix 2. Fraud Resources

General Consumer Complaints

Agency	Website	Phone Number
Better Business Bureau	www.bbb.org	Use zip code to find 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

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.	1–877–908–3360
AARP Fraud Watch Network	www.aarp.org/fraudwatchnetwork	1–800–646–2283
Local/State AG Office	http://www.naag.org/current-attorneys-general.php	1–202–326–6000
U.S. Senator or Representative for Constituent Casework.	http://www.senate.gov/general/contact__information/senators__cfm.cfm. http://www.house.gov/	1–202–224–3121 (Capitol Switchboard)
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/	General: 1–202–872–0888
IRS Scam Reporting Hotline	https://www.treasury.gov/tigta/contact__report__scam.shtml.	1–800 366–4484
HHS OIG	http://www.hhs.gov/grants/grants/avoid-grant-scams/index.html.	1–800–447–8477
National Center for Victims of Crime.	https://www.victimsofcrime.org/	1–855–484–2846
FINRA Securities Helpline for Seniors.	http://www.finra.org/investors/finra-securities-helpline-seniors.	1–844–574–3577
Center for Elder Rights Advocacy	http://www.legalHotlines.org/legal-assistance-resources.html.	1–866–949–2372

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	http://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.	1–866–949–2372

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 (Do not call registry)
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 (report suspected Medicare fraud related to Medical ID theft: 1–800–447–8477

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	1–877–777–4778
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	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

Sweepstakes Scams

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 (press 5 for more options then 5 for fraud/suspicious activity)
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	

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

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.	http://www.hud.gov/offices/hsg/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 the victim's 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

Agency	Website	Phone Number
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	

Attorneys General

- **Alabama**
  (334) 242-7300
- **Alaska**
  (907) 465-3600
- **Arizona**
  (602) 542-4266
- **Arkansas**
  (800) 482-8982
- **California**
  (916) 445-9555
- **Colorado**
  (720) 508-6022
- **Connecticut**
  (860) 808-5318
- **Delaware**
  (302) 577-8338
- **District of Columbia**
  (202) 724-1305
- **Florida**
  (850) 414-3300
- **Georgia**
  (404) 656-3300
- **Hawaii**
  (808) 586-1500
- **Idaho**
  (208) 334-2400
- **Illinois**
  (312) 814-3000
- **Indiana**
  (317) 232-6201
- **Iowa**
  (515) 281-5164
- **Kansas**
  (785) 296-2215
- **Kentucky**
  (502) 696-5300
- **Louisiana**
  225-326-6000
- **Maine**
  (207) 626-8800
- **Maryland**
  (410) 576-6300
- **Massachusetts**
  (617) 727-2200
- **Michigan**
  (517) 373-1110
- **Minnesota**
  (651) 296-3353
- **Mississippi**
  (601) 359-3680
- **Missouri**
  (573) 751-3321
- **Montana**
  (406) 444-2026
- **Nebraska**
  (402) 471-2682
- **Nevada**
  (775) 684-1100
- **New Hampshire**
  (603) 271-3658
- **New Jersey**
  (609) 292-8740
- **New Mexico**
  (505) 827-6000
- **New York**
  (518) 474-7330
- **North Carolina**
  (919) 716-6400
- **North Dakota**
  (701) 328-2210
- **Ohio**
  (614) 466-4320
- **Oklahoma**
  (405) 521-3921
- **Oregon**
  (503) 378-4400
- **Pennsylvania**
- (717) 787-3391
- **Puerto Rico**
  (787) 721-2900
- **Rhode Island**
  (401) 274-4400
- **South Carolina**
  (803) 734-3970
- **South Dakota**
  (605) 773-3215
- **Tennessee**
  (615) 741-3491
- **Texas**
  (512) 463-2100
- **Utah**
  (801) 538-9600
- **Vermont**
  (802) 828-3173
- **Virginia**
  (804) 786-2071
- **Washington**
  (360) 753-6200
- **West Virginia**
  (304) 558-2021
- **Wisconsin**
  (608) 266-1221
- **Wyoming**
  (307) 777-7841

ENDNOTES

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

[3] TIGTA Conference Call with Aging Committee. January 7, 2016.

[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.

[5] Internal Revenue Service. Tax Scams/Consumer Alerts. *https://www.irs.gov/uac/Tax-Scams-Consumer-Alerts* (accessed January 21, 2016).

[6] TIGTA Conference Call with Aging Committee. January 7, 2016.

[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* (accessed January 21, 2016).

[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* (accessed January 18, 2016).

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

[10] Federal Trade Commission. Consumer Information: Prize Scams. *http://www.consumer.ftc.gov/articles/0199-prize-scams* (accessed January 18, 2016).

[11] Federal Trade Commission. 2015. *Consumer Sentinel Network Data Book* for January-December 2014. (February): 79

[12] 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.

[13] 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 18, 2016).

[14] 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 18, 2016).

[15] 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 21, 2016).

[16] U.S. Senate, 876–SCAM, S. 6–7.

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

[18] 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.

[19] Citation needed for the testimony of the fraud case victim

[20] 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* (accessed January 21, 2016).

[21] Federal Trade Commission. FTC Announces Robocall Challenge Winners. *https://www.ftc.gov/news-events/press-releases/2013/04/ftc-announces-robocall-challenge-winners* (accessed January 21, 2016).

[22] Ibid.

[23] 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* (accessed January 21, 2016).

[24] 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* (accessed January 18, 2016).

[25] 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* (accessed January 21, 2016).

[26] 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* (accessed January 18, 2016).

[27] 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.

[28] Ibid.

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

[30] Federal Bureau of Investigation. Internet Crime Complaint Center. 2015. 2014 *Internet Crime Report.* (May 9): 4.

[31] Ibid., 9.

[32] U.S. Senate, *Virtual Victims.*

[33] Ibid., S. 18.

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

[35] 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* (accessed January 18, 2016).

[36] FTC, Consumer Sentinel Network Data Book, 14.

[37] Ibid.

[38] Ibid., 12.

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

[40] Medicare Access and CHIP Reauthorization Act of 2015. Public Law 114 10. 114th Congress, 2nd sess.

[41] 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.

[42] Ibid., S. 12 15 and S.17 20.

[43] FTC, *Consumer Sentinel Network Data Book,* 82.

[44] 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

[45] Elton, Catherine. 2012. The Fleecing of America's Elderly. *Consumers Digest.* November 10.

[46] 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).

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

[48] Ibid., 14.

[49] Ibid., 15.

[50] 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).

[51] 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.

[52] Ibid.

[53] Ibid., 10.

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

[55] 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).

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

[57] The Patient Protection and Affordable Care Act, Subtitle H. Public Law 111–148. 111th Congress, 2nd sess.

[58] GAO, Elder Justice, 22.

[59] Ibid., 25 26

[60] U.S. Congress. *Congressional Record.* 2015. 114th Cong., 1st sess. S7595–S7596.

[61] 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).

[62] U.S. Congress. Senate. 2015. *Broken Trust: Combating Financial Exploitation of Vulnerable Seniors: Hearing before the Special Committee on Aging.* 114th Congress, 1st sess., February 4. S. 63

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

[64] Ibid.

[65] U.S. Senate, *Broken Trust.*

[66] Eligon, John. 2015. Brooke Astor's Son Guilty in Scheme to Defraud Her. *New York Times.* October 8.

[67] FTC, *Consumer Sentinel Network Data Book,* 77

[68] Ibid., 79.

[69] Ibid., 6 and 79.

[70] Shadel, Doug and David Dudley. 2015. A con man steals one woman's heart—and $300,000. Here's how it happened. *AARP the Magazine.* June/July.

[71] FBI, 2014 Computer Crime Report, 15.

[72] Federal Trade Commission. Consumer Information: Online Dating Scams. *http://www.consumer.ftc.gov/articles/0004-online-dating-scams* (accessed January 18, 2016).

[73] 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* (accessed January 18, 2016).

[74] FBI, 2014 Computer Crime Report, 42.

[75] Ibid.

[76] 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/* (accessed January 18, 2016).

[77] Halpern, Mollie. "Podcast and Radio: Romance Scams." FBI This Week. *https://www.fbi.gov/news/podcasts/thisweek/romance-scams.mp3/view* (accessed January 18, 2016).

[78] Office of the Indiana Attorney General. Home Improvement Scams. *http://www.in.gov/attorneygeneral/2545.htm* (accessed January 18, 2016).

[79] FTC, *Consumer Sentinel Network Data Book,* 6.

[80] Federal Trade Commission. Consumer Information: Dealing with Weather Emergencies. *http://www.consumer.ftc.gov/features/feature-0023-weather-emergencies* (accessed January 18, 2016).

[81] Federal Trade Commission. Consumer Information: House alarms can't stop scammers. *https://www.consumer.ftc.gov/blog/house-alarms-cant-stop-scammers* (accessed January 18, 2016).

[82] Ibid.

○