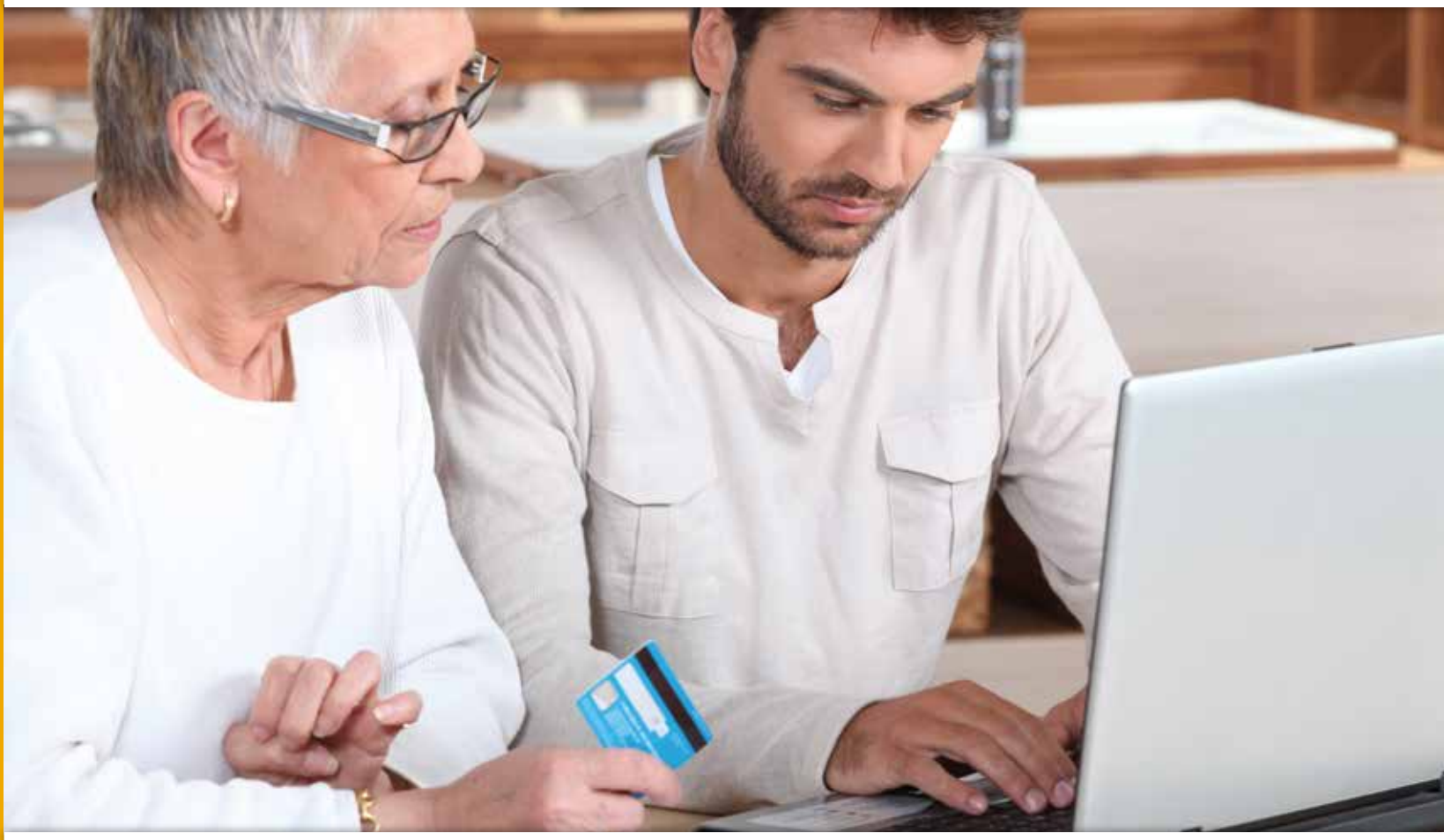
United States Senate
Special Committee on Aging

Fighting Fraud:



Senate Aging Committee Identifies Top 10 Scams Targeting Our Nation's Seniors

Senator Susan M. Collins (R-ME), Chairman

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

Tips from the United States Senate Special Committee on Aging for

Avoiding Scams

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

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

Table of Contents

Dear Friends:

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

The U.S. Senate Special Committee on Aging has made consumer protection and fraud prevention a major focus of its work. In recent years, the Committee has held hearings examining telephone scams, tax-related schemes, Social Security fraud, and the implications of payday loans and pension advances for seniors, among other issues. The Committee maintains a toll-free Fraud Hotline: **1-855-303-9470**. By serving as a resource for seniors and others affected by scams, the Hotline has helped increase reporting and awareness of consumer fraud.

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

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

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

Over the past year, more than 2,200 individuals in all 50 states and the District of Columbia have contacted the Fraud Hotline — more than double the number of calls received in 2015.

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 work with us to fight fraud.

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

The range and frequency of scams perpetrated against seniors that were reported to the Fraud Hotline in 2016 demonstrate the extent of this epidemic. In 2017, the Aging Committee intends to build on its successful efforts to investigate and stop scams aimed at our nation's seniors and ensure that federal agencies are aggressively pursuing the criminals who commit these frauds.

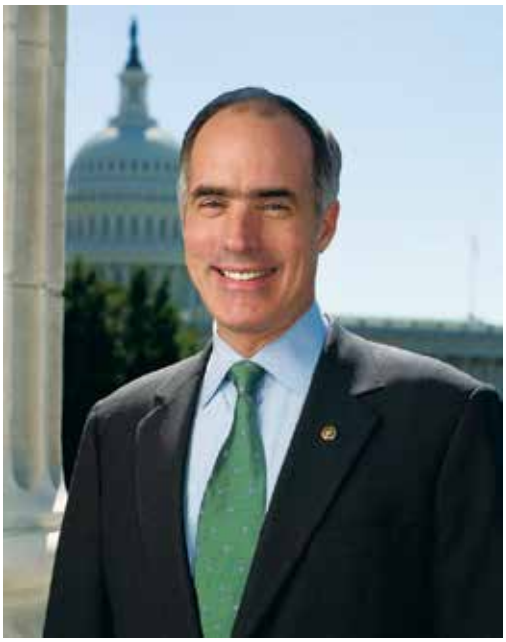
Sincerely,

Susan M. Collins

Chairman

Robert P. Casey Jr.

Ranking Member



Executive Summary

From January 1, 2016, through December 31, 2016, the Senate Aging Committee's Fraud Hotline received a total of 2,282 complaints from residents in all 50 states and the District of Columbia. Calls pertaining to the top 10 scams featured in this report accounted for more than 90 percent of the complaints.

The top complaint, the focus of more than twice as many calls as any other scam, involves seniors who receive calls from fraudsters posing as agents of the Internal Revenue Service (IRS). These criminals falsely accuse seniors of owing back taxes and penalties in order to scam them. Due to the extremely high call volume, 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.

The third most common scam reported to the Hotline involved robocalls or unwanted phone calls. On June 10, 2015, the Aging Committee held a hearing on the increase in these calls that are made despite the national Do-Not-Call registry. The Committee examined how the rise of new technology has made it easier for scammers to contact and deceive consumers and has rendered the Do-Not-Call registry ineffective in many 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.

Elder financial abuse was fifth 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 M. Collins, former Ranking Member Claire McCaskill, and current Ranking Member Robert P. Casey Jr. have introduced the *Senior$afe Act of 2017*, which would allow trained financial services employees to report suspected cases of financial exploitation to the proper authorities without concern that they would be sued for doing so. The Committee also

examined the financial abuse by guardians and other court appointed fiduciaries at a hearing in November 2016.

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.

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

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.

Counterfeit check scams were the ninth most common scam reported to the Fraud Hotline. In these cases, scammers trick victims into cashing or depositing a check, and then wiring the money to back to the fraudsters. The victim eventually learns from his or her bank that the check bounced and they are liable for the funds.

Identity theft rounded out the top 10 scams reported to the Fraud Hotline in 2016. 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 requiring the removal of seniors' Social Security numbers from their Medicare cards, which will help prevent identity theft.

Key Figures

Rank	Type of Scam	# of Complaints
1	IRS Impersonation Scams	1680
2	Sweepstakes Scams/Jamaican Lottery	124
3	Robocalls/Unwanted Phone Calls	92
4	Computer Scams	77
5	Elder Financial Abuse	53
6	Grandparent Scams	39
7	Romance Scams	36
8	Government Grant Scams	35
9	Check Scams	23
10	Identity Theft	15

Figure 1. Top 10 Scams Reported to Aging Committee Fraud Hotline from January 1, 2016, to December 31, 2016. [1]

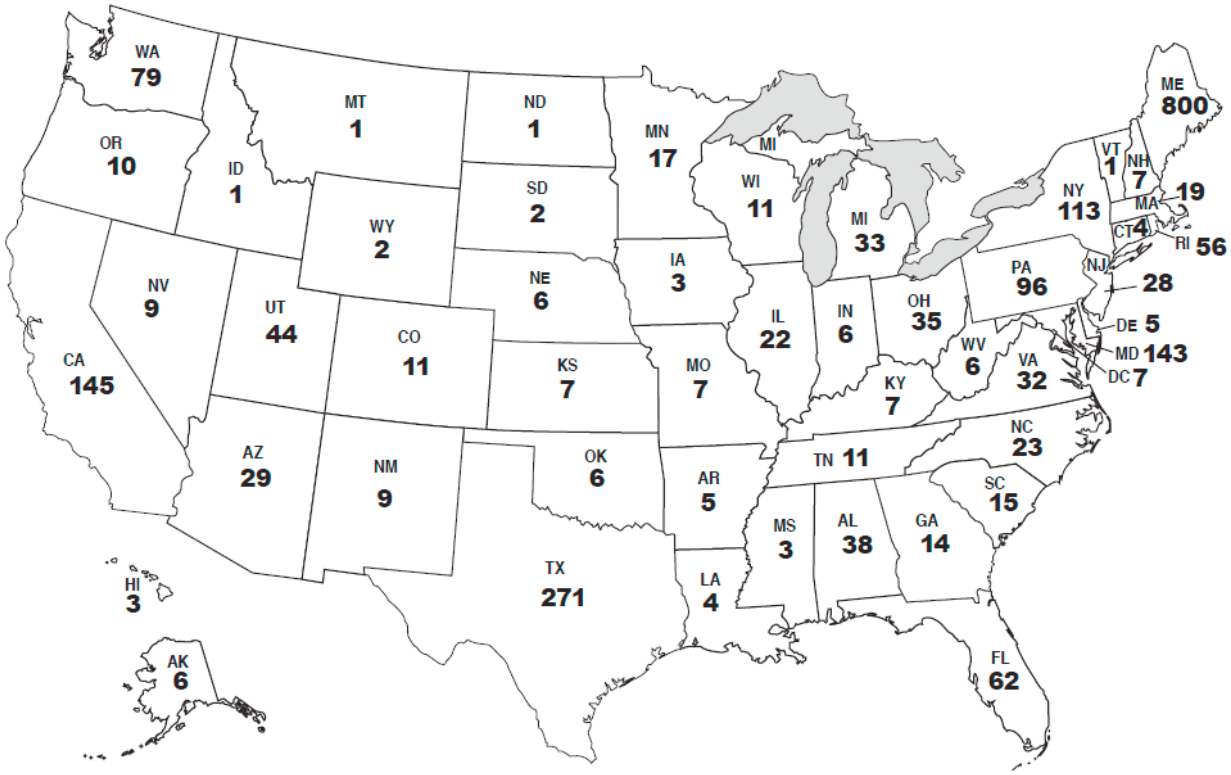


Figure 2. Origin of Calls Received by the Aging Committee's Fraud Hotline from January 1, 2016, to December 31, 2016. [2]

[1] Please see Appendix 1 for a full list of scams reported to the Fraud Hotline in 2016.
[2] Please see Appendix 1 for a table of the underlying data.

Abbreviations

Adult Protective Services	APS
Department of Homeland Security	DHS
Department of Justice	DOJ
Federal Communications Commission	FCC
Federal Trade Commission	FTC
Financial Industry Regulatory Authority	FINRA
Government Accountability Office	GAO
Health insurance claim number	HICN
Internal Revenue Service	IRS
Internet Crime Complaint Center	IC3
Social Security Number	SSN
Treasury Inspector General for Tax Administration	TIGTA
Voice over Internet Protocol	VoIP

Top Ten Scams Reported to the Senate Aging Committee's Fraud Hotline in 2016

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, at least 1.87 million Americans have been targeted by scammers impersonating IRS officials, with 20,000 to 40,000 people submitting complaints on this scam every week, with an average of 150 to 200 victims a week.[2] Additionally, more than 10,000 Americans have lost a total more than $54 million from this scam.[3] The IRS impersonation scam was the most frequent scam reported to the Fraud Hotline in 2016.

In response to the initial 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 steps individuals should take if they receive a call.[5]

TIGTA data suggests that increased public awareness has made a difference and harder for criminals to find victims.[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. In April 2016, TIGTA announced that it began receiving an influx of complaints that IRS impersonators were demanding payment in the form of iTunes gift cards.[9] At the same time, the Committee's Fraud Hotline also began receiving reports from callers that scammers were demanding payments via gift cards. The criminals tell victims that if they immediately pay the amount that is allegedly owed, the issue with

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

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 "spoofed" their phone numbers to make it appear as though they are calling from a local law enforcement agency. When the unsuspecting victims see the "Internal Revenue Service" or the name of the local police department appear on their caller IDs, they are understandably concerned and are often willing to follow the supposed government official's instructions in order to resolve the alleged tax issue.

Fraud Case #1:

"Mike," from Texas, called the Fraud Hotline after realizing that he had been scammed out of $1,800. Mike said that he received a call from someone claiming to work for the IRS. The alleged agent told Mike that he would be arrested unless he paid his overdue taxes immediately. The scammer directed him to go to a local grocery store and purchase iTunes gift cards. After purchasing the gift cards, Mike read the numbers on the back of the cards to the person on the phone whom he believed was an IRS agent. This allowed the scammer to steal the funds on the cards. Mike did not realize he had been scammed until later that day when he told his daughter about the phone call. A Fraud Hotline investigator filed a report with TIGTA on Mike's behalf.

As of January 27, 2017, the Department of Justice (DOJ) had only obtained convictions of five 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.[10]

In 2016, TIGTA and DOJ made progress arresting and charging more criminals for their role in this pervasive scam. Because of a tip reported to the Committee's Fraud Hotline, in May 2016, TIGTA arrested five individuals in Miami, Florida, connected with the IRS impersonation scam. Two individuals were identified as a direct result of the crucial information provided by a fraud investigator with the Aging Committee's Hotline. According to the court documents, the suspects were responsible for almost $3 million in schemes that allegedly defrauded more than 1,200 victims.[11]

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

The Fraud Hotline investigator who received the victim's report was able to trace the wire transfer to Minnesota and reported this information to TIGTA. TIGTA sent agents to Minnesota, pulled surveillance tapes, and quickly identified two suspects. TIGTA's investigation led them to identify three additional suspects.[12] Law enforcement arrested all five suspects and subsequently charged them with wire fraud and conspiracy to commit wire fraud.[13] At the time, this was the largest single law enforcement action in the history of the IRS impersonation scam.[14]

On September 15, 2016, TIGTA and the DOJ announced that two residents of Bristol, Connecticut, were arrested for participating in the IRS impersonation scam. According to court documents, between October 2015 and May 2016, the alleged criminals received approximately $547,000 in wired funds.[15] One of the two criminals arrested allegedly received approximately $40 per transaction and made approximately $500 per day.[16]

Fraud Case #2:

"Jill," from Maine, lost $8,700 to criminals posing as IRS agents. Local police received an anonymous tip about a woman buying a large amount of iTunes gift cards. When the police arrived, they found Jill in her car in the store parking lot, talking on her phone, and a pile of gift cards on the passenger's seat. Jill, afraid the police were there to arrest her, told them that she was on the phone paying her IRS bill. Recognizing the scam, the police officer told her to immediately hang up the phone. While the police stopped her from reading more card numbers to the criminals, Jill had already lost $8,700. The police officers took a report and encouraged her to contact the Aging Committee's Fraud Hotline. A Fraud Hotline investigator reported the case to TIGTA and Apple. Unfortunately, Apple was unable to recover the funds by the time the incident was reported.

The largest enforcement action came on October 27, 2016, when TIGTA and DOJ announced that after an exhaustive three-year joint investigation, 20 individuals were arrested in the United States and 32 individuals and five call centers in India were charged for their alleged involvement in the scam.[17] Following this crack down, both TIGTA and the Committee's hotline noticed a decline in the number of IRS scam cases being reported. During the scam's peak, TIGTA was receiving between 20,000 and 40,000 complaints a week, with an average of 150 to 200 victims a week. In December 2016, however, TIGTA reported receiving less than 2,000 calls a week, with fewer than 15 victims a week.[18] During the second week of January 2017, TIGTA reported that it received just eight new reports of victims losing money to this scam.[19] TIGTA believes this substantial drop-off is due, in part, to the recent indictments of Indian call center operators in October.

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

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.[20] According to the Federal Trade Commission (FTC) the number of sweepstakes scams increased by 42.98 percent between 2013 and 2015.[21]

During the 113th Congress, the Aging Committee launched an investigation of the Jamaican lottery scam, one of the most pervasive sweepstakes scams.[22] 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.[23]

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.[24] Several convictions have been made obtained in connection with this scam. In November 2015, a 25-year-old Jamaican national living in the United States was sentenced to 20 years in prison after being found guilty of selling lists of potential victims, referred to as "lead lists."[25]

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.

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

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.[26] Criminals once involved in narcotics

trafficking have found these scams to be safer and more lucrative.

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:

"John," from New Jersey, called the Fraud Hotline to report that he had been a victim of a sweepstakes scam. John said he received a phone call alerting him that he had won $2.5 million and a brand new car. In order to receive his winnings, however, John was told to pay the taxes and associated fees. Over a span of four days, John sent ten wire transfers totaling more than $100,000. A Fraud Hotline investigator filed a report with the wire transfer company and the Federal Trade Commission. In addition, the investigator gave John information and tips to help prevent him from being scammed again.

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.[27] Unfortunately, 13 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. In fiscal year 2016, the Federal Trade Commission (FTC) received 5.34 million Do-Not-Call registry complaints, an increase of 49.22 percent from the previous year.[28]

Robodialers can be used to distribute pre-recorded messages or to connect the person who answers the call with a live person. 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 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.

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

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

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..

Robocalling allows scammers to maximize the number of individuals and households they can reach.

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."*[29] By using an inexpensive smartphone app, the staff member was able to make it appear that the calls were from the Internal Revenue Service 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.[30]

In response to the high volume of robocalls that are made in violation of the national Do-Not-Call registry, the FTC launched a contest in October 2012 to identify innovative solutions to protect consumers from these calls.[31] 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.[32]

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.

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.[33] 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.[34] In this context, a

honeypot is an information system that attracts robocalls so that researchers can analyze them and develop preventive techniques.[35] 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.[36] 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.[37]

Fraud Case #5

"Mason", from Maryland, called to report receiving multiple, unsolicited, robocalls about an opportunity to improve his credit score. A Fraud Hotline investigator filed a report with the Federal Trade Commission and the Do-Not-Call Registry on his behalf. The investigator also encouraged Mason to contact his telephone company and request that it block the phone number to avoid unwanted calls in the future.

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 began seeing 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.[38] The company estimated that 3.3 million Americans are victims of technical support scams annually, with losses of roughly $1.5 billion per year.[39] 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.[40] In addition, in 2015, the Internet Crime Complaint Center (IC3), a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center, received 288,012 computer crime complaints with a loss of $1,070,711,522.[41] Americans age 60 and older accounted for 18.01 percent of these complaints.[42] In 2015, the Federal Trade Commission (FTC) received 39,924 complaints of Tech Support Scams, a 38,661 percent increase from the year before.[43]

Fraud Case #6:

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.

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."*[44] The hearing featured representatives from Microsoft and the FTC who spoke about the challenges in combating this fraud given its many variations and constant changes.[45]

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 "sponsored results." The FTC found that a network of scammers paid Google more than one million dollars since 2010 for advertisements and for certain key search terms.[46] 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.[47]

Fraud Case #7:

"Anne," from California, called the Committee's Fraud Hotline to report that she had been the victim of a computer tech support scam. She explained that she received a call from someone claiming to work for a Microsoft and that there was an issue with her computer. Anne had recently purchased a new computer; therefore, she thought the call was legitimate. The caller instructed her to go to her computer and, with Anne's assistance, the caller was able to access it. The caller offered to remotely repair the computer for $199, which Anne agreed to pay using her credit card. After ten minutes, the caller said he had fixed the computer. The next day, Anne received another call from someone also claiming to be a Microsoft employee. He told her that there was another issue with her computer. Anne now suspected that she had been scammed and she called the Fraud Hotline. An investigator filed a report with the Federal Trade Commission, the FBI's Internet Crime Complaint Center, and Microsoft. The investigator also encouraged Anne to dispute the credit card charge as fraud.

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 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.[48] One study found that, for every case of financial fraud that is reported, as many as 14 go unreported.[49] 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.[50]

The Fraud Hotline documents complaints of elder abuse and refers callers to local jurisdiction's 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.[51] APS can also refer cases to law enforcement agencies or district attorneys for criminal investigation and prosecution.[52] 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.[53]

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.[54] Most victims are between the ages of 80 and 89, live alone, and require support with daily activities.[55] 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.[56]

Victims whose assets were 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.[57] Few civil attorneys, however, are trained in issues related to older victims and financial exploitation.[58] 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.[59]

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.[60] The law formed the Elder Justice Coordinating Council, which first convened on October 11, 2012, and is tasked with increasing cooperation among federal agencies.[61] 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.[62]

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. Aging Committee Chairman Susan Collins and former Ranking Member Claire McCaskill have introduced the *Senior$afe Act*, a bipartisan bill cosponsored by Ranking Member Robert P. Casey Jr. and others, which would provide certain individuals with immunity for disclosing suspected financial exploitation of senior citizens.[63] The Financial Industry Regulatory Authority is simultaneously pursuing rulemaking that would empower financial professionals to protect their senior clients from financial abuse.[64]

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.[65] 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.[66]

In March 2016, an attorney in Belfast, Maine was sentenced to 30 months in prison for bilking two elderly female clients out of nearly a half a million dollars over the course of several years.[67] The lawyer's brazen theft was uncovered when a teller at a local bank noticed that he was writing large checks to himself on his clients' accounts.[68] When confronted by authorities, he offered excuses that the prosecutor later described as "breathtaking."[69] For example, according to the *Bangor (Maine) Daily News*, he put one of his clients into a nursing home to recover from a temporary medical condition, and then kept her there for four years until the theft of her funds came to light. Meanwhile, he submitted bills for "services," sometimes totaling $20,000 a month, including charging her $250 per hour for six to seven hours to check on her house, even though his office was just a one-minute drive down the road.[70]

Another tragic case of theft and abuse was featured in a November 2016, *Maine Sunday Telegram* article. The article detailed the story of an elderly woman from Los Angeles, California, who went missing in 2008.[71] In 2012, authorities found her, alive but in poor health, abandoned in a tiny cabin in Maine by three people who had "befriended" her years earlier. After gaining the woman's trust, and control of her finances, these criminals sold her house and stole her money, cheating her of an estimated $1 million in assets.[72] Today, this 90-year-old woman is a ward of the state and lives in a nursing home in rural Maine – thousands of miles away from the life she used to know.[73]

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.

Fraud Case #8

"Christopher", from Arizona, called the Committee's Fraud Hotline to report that he suspected that his brother was stealing money from his elderly mother. Christopher explained that his mother is suffering from dementia and that his brother told her go to the bank and deposit checks into his account. The Fraud Hotline investigator encouraged Christopher to file a complaint with the Arizona Attorney General's office and adult protective services.

In November 2016, the Aging Committee examined financial abuse committed by guardians and other court appointed fiduciaries. During the hearing, titled, "*Trust Betrayed: Financial Abuse of Older Americans by Guardians and Others in Power*", the Committee released a new GAO report on guardianship abuse. The report builds on a 2010 study which found hundreds of cases of abuse, neglect, and exploitation and identified $5.4 million that had been improperly diverted.[74] The updated report examined cases of elder financial abuse over a four-year period, from 2011 to 2015, and examined measures taken by several states to help protect older adults with guardians.

According to the GAO, guardianship abuse is widespread, but it remains difficult to determine the extent of elder abuse by guardians nationally due to limited data. GAO noted that some progress is being made to collect data on guardianships and improve the guardianship process. In 2013, the Department of Health and Human Services (HHS) began developing the National Adult Mistreatment Reporting System (NAMRS) to provide consistent and accurate national data on senior abuse. HHS has completed the pilot project and expects to roll out the system in 2017.

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

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

Another witness, Jaye Martin, the Executive Director of Legal Services for the Elderly (LSE) in Maine, testified that her organization assisted 260 victims of elder abuse during the last 12 months. This was a 24 percent increase from the prior year. While this number includes physical and emotional abuse as well, roughly half of the cases handled by LSE involved financial exploitation of seniors. Even more alarming was Ms. Martin's testimony that in 75 percent of those cases, the financial exploitation was carried out by a family member. Unfortunately, these numbers only represent the tip of the iceberg, since so many abuse cases go unreported. Victims are often ashamed or afraid to alert authorities about financial exploitation, particularly when it involves a family member.

Fraud Case #9

After watching the Committee's hearing on financial exploitation by guardians, "Mary," from Oregon, called to report that she suspected her 91-year old mother was being financially exploited through a guardianship. Mary began suspecting financial exploitation once the caretaker started significantly reducing the amount of time Mary and her siblings could visit their mother. A Fraud Hotline investigator shared with Mary that she should report the suspected abuse to the Oregon Attorney General's office and Adult Protective Services as they have jurisdiction over these cases.

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 their family member was pulled over by the police and arrested after drugs were found in the car. The scammer who is pretending to be the victim's grandchild will often tell the victim to refrain from alerting the grandchild's parents. The scammer then asks the victim to help by sending money in the fastest way possible. This typically requires the victim to go to a local retailer and send an 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.

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 2015, the Federal Trade Commission (FTC) received 10,565 complaints of individuals impersonating friends and family members, down from 14,525 in 2014.[75] 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.[76]

Fraud Case #10

"Phil," a bank employee in Connecticut, called the Fraud Hotline to report that one of his clients was attempting to wire $30,000 to Mexico. The customer told Phil that his grandson had been arrested following a car accident and now needed to be bailed out of jail. Phil suspected fraud and didn't grant the customer's request. Phil called the Fraud Hotline. An investigator called Phil's client and convinced him he was being scammed. The Fraud Hotline investigator filed a complaint with the local police department, the Federal Trade Commission, and the Department of Homeland Security.

7 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.[77] 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. In 2016, romance scams and confidence fraud increased in frequency from the previous year. As a result, romance scams and confidence fraud moved up to the seventh most reported scam to the Committee's hotline. 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.[78] Con artists have been

Fraud Case #11

"Sara," from Maine, contacted the Fraud Hotline to report that she had lost nearly $32,000 to a man she fell in love with on Facebook. Sara told a Fraud Hotline investigator that she received a Facebook message from someone claiming to be a soldier stationed in Afghanistan. After exchanging messages for a couple a weeks, she said the two fell in love. Eventually, the man began asking for money to help cover a wide range of expenses including: cell phones, phone cards, and even medical care after he had supposedly been injured. Sara became suspicious when he said he missed his flight back to the United States and needed more money. Sara provided the investigator with copies of the wire transfers. The investigator filed reports with the wire transfer company and the Federal Trade Commission. In addition, the investigator reported the fraudulent profile to Facebook.

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

Inevitably, con artists in these scams will ask their victims for money for a variety of things. Often 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.[79] 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.[80]

In 2015, the FBI's IC3 received 12,509 complaints about romance and confidence scams that cost victims $203,390,531, the second highest type of scam by victim loss reported to the IC3.[81] In comparison, in 2014 the IC3 received 5,883 complaints about romance and confidence scams that cost victims $86.7 million dollars.[82] Nearly half of the victims in 2014 were age 50 or older, and this group accounted for approximately 70 percent of the money lost to this scam last year.[83] Romance and confidence scams disproportionally target women, usually between the ages of 30 and 55 years old.[84] Unfortunately, both the amount of financial loss and the number of complaints for this crime have increased in recent years.[85]

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

8 Government 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." 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."[86] According to FTC data, the frequency of Americans reporting grant scams has dropped over the past three years.[87] In 2015, the FTC received 4,077 complaints, which was about a 50 percent decrease from the prior year.[88]

Fraud Case #12

"Bethany," from Pennsylvania, called the Fraud Hotline to report that she had fallen victim to a government grant scam. Bethany explained that she received a call from the "Federal Grant Office" regarding a $60,000 "Housing Opportunities Grant" for which she qualified. In order to receive the money, however, Bethany was told to send a check for $4,200 to pay taxes and processing fees. Bethany never received the "grant," and realized she had been scammed. She contacted her bank, but the criminals had already cashed her check. A Fraud Hotline investigator reported this to the Federal Trade Commission and the U.S. Postal Inspector.

Fraud Case #13

"Audrey," from Maryland, reported a Facebook message alerting her to an opportunity to receive a federal grant. In order to receive the grant, however, she had to pay $9,000 in fees and taxes. Audrey knew immediately that this was a scam and she called the Fraud Hotline. An investigator reported the fraudulent message to Facebook, the Federal Trade Commission, and the FBI's Internet Crime Complaint Center.

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 Counterfeit Check Scams

While this scam is not new, the Committee's Fraud Hotline saw a significant increase in counterfeit check scams in 2016. According to the Federal Trade Commission (FTC), fake checks are printed with the names and addresses of legitimate financial institutions, and can even have real account and routing numbers.[89] The FTC warns that some checks look so authentic that even bank tellers can be fooled.[90] In 2015, the FTC received 14,424 complaints of counterfeit check scams, an 11.47 percent increase from the previous year. In 2014, the U.S. Postal Inspection Service (USPIS) confiscated and stopped 35,000 fake checks, totaling more than $40 million, from reaching victims.[91]

While there are numerous variations of this type of scam, fake check scams always involve someone giving you a genuine-looking check or money order and asking you to wire money somewhere in return.[92] According to the FTC, under federal law, banks generally must make funds available from U.S. Treasury checks, most other governmental checks, and official bank checks (cashier's checks, certified checks, and teller's checks) one business day after the check is deposited. For other checks, banks must make the first $200 available the day after the check is deposited, and the remaining funds must be made available on the second business day after the deposit.[93] The Consumer Federation of America warns that consumers often do not realize the check is counterfeit until it is deposited or cashed and the money is wired.[94] Below are several of the most common variations of this scam:

- **Foreign Lottery Scams.** Foreign lottery scams, or sweepstakes scams, involve scammers contacting potential victims, either by phone or mail, and informing them that they have won a lottery. Scammers then require the victims to pay a fee to either collect their supposed winnings or improve their odds of winning the prize.[95] What is unique to the counterfeit check scam angle is that often times scammers will mail victims a fake check to help cover the fees. They will instruct the victim to cash or deposit the check into their bank accounts and then wire the money back to them. Usually within a couple days, the victim learns from their bank that the check was counterfeit.

Fraud Case #14

"Mark," from Michigan, contacted the Fraud Hotline to report receiving numerous checks in the mail that "clearly appeared to be fake." While Mark did not lose any money, the Fraud Hotline investigator reported the checks to the Federal Trade Commission and the U.S. Postal Inspector.

- **Check Overpayment and Internet Auction Scams.** In this deviation of the scam, some scammers target victims through classified ads and online auction sites. Scammers agree to purchase a listed item and send either a fake cashier's check, corporate check, or personal check to listed seller. The FTC explains that the scammer usually comes up with a reason for writing the check for more than the purchase price, and will ask the seller to wire back the difference after depositing the check.[96] Unfortunately, the victim will learn the check was bad only after sending the scammer the difference. By this time, it is too late and the victim is liable for the entire amount.[97]

- **Secret Shopper Scams.** In this version of the scam, a victim is hired to be a "secret shopper" and asked to evaluate a particular money transfer service.[98] Scammers mail the victim a check and instruct them to cash it and take the cash to the specified money transfer service. In order to give the scam more credibility, the FTC explains that victims are supposed to evaluate their experience, however, no one collects or reads the evaluation.[99] Like other versions of counterfeit check scams, the victim doesn't learn that this is a scam until it's too late, and they are told by their bank that the check bounced and they are responsible for the amount.

Law enforcement has recently taken positive steps in combatting this type of scam. In September 2016, The Treasury Department's Office of Foreign Assets Control (OFAC) and the USPIS both took action against PacNet Services Ltd., an international payments processor and money services business based in Vancouver, Canada, along with affiliate companies and their operators.[100] OFAC designated the company a significant trans-national criminal organization, meaning its property was frozen. OFAC is also designating a global network of 12 individuals and 24 entities across 18 countries a transnational criminal organization.

Fraudsters are known to use payment processors to help shield their operations from authorities, since banks will shut down accounts or report them to authorities if they detect suspicious activity, like a high number of small deposits, complaints or refunds.[101] According to the Department of Justice (DOJ), in 2016 alone, PacNet processed payments for the perpetrators of more than 100 different mail fraud campaigns, collectively involving tens of millions of dollars.[102] In doing so, PacNet provided fraudsters in other countries with unfettered access to U.S. banks.

Also in September 2016, DOJ filed a criminal complaint in the U.S. District Court for the Eastern District of New York, against Ercan Barka, 34, a resident of Turkey, with conspiracy to commit mail fraud.[103] Mr. Barka is accused of arranging for fraudulent solicitations to be mass-mailed to victims across the United States.[104] The fraudulent solicitations told recipients that they had won cash awards or lavish prize items and needed to pay a "fee" to claim their winnings.[105] Victims allegedly received nothing in return for their fees.[106] U.S. Postal Inspectors arrested Mr. Barka at JFK International Airport in New York as he was about to board a plane bound for Turkey.[107]

Fraud Case #15

"Sherri," from Pennsylvania, contacted the Fraud Hotline to report receiving a check in the mail for $3,950. Along with the check was a letter informing her that if she deposited the check and mailed out a new check in the same amount to an address in South Africa, she would receive $250,000. A Fraud Hotline investigator explained to Sherri that this was a scam and filed a report with the Federal Trade Commission and the US Postal Inspector on her behalf.

FTC's Tips on How to Protect Yourself from Counterfeit Check Scams:

- Throw away any offer that asks you to pay for a prize or a gift. If it's free or a gift, you shouldn't have to pay for it. Free is free.
- Resist the urge to enter foreign lotteries. It's illegal to play a foreign lottery through the mail or the telephone, and most foreign lottery solicitations are phony.
- Know who you're dealing with, and never wire money to strangers.
- If you're selling something, don't accept a check for more than the selling price, no matter how tempting the offer or how convincing the story. Ask the buyer to write the check for the correct amount. If the buyer refuses to send the correct amount, return the check. Don't send the merchandise.
- As a seller, you can suggest an alternative way for the buyer to pay, like an escrow service or online payment service. There may be a charge for an escrow service. If the buyer insists on using a particular escrow or online payment service you've never heard of, check it out. Visit its website, and read its terms of agreement and privacy policy. Call the customer service line. If there isn't one — or if you call and can't get answers about the service's reliability — don't use the service.
- If you accept payment by check, ask for a check drawn on a local bank, or a bank with a local branch. That way, you can make a personal visit to make sure the check is valid. If that's not possible, call the bank where the check was purchased, and ask if it is valid. Get the bank's phone number from directory assistance or an Internet site that you know and trust, not from the check or from the person who gave you the check.
- If the buyer insists that you wire back funds, end the transaction immediately. Legitimate buyers don't pressure you to send money by wire transfer services. In addition, you have little recourse if there's a problem with a wire transaction.
- Resist any pressure to "act now." If the buyer's offer is good now, it should be good after the check clears.

Source: https://www.consumer.ftc.gov/articles/0159-fake-checks#Youandyourbank

10 Identity Theft

Identity thieves not only disrupt the lives of individuals by draining bank accounts, making unauthorized credit card charges, and damaging credit reports, but they also often defraud the government and taxpayers by using stolen personal information to submit fraudulent billings to Medicare or Medicaid or apply for and receive Social Security benefits to which they are not entitled. Fraudsters also use stolen personal information, including Social Security numbers (SSN), to commit tax fraud or to fraudulently apply for jobs and earn wages. According to the Federal Trade Commission (FTC), government documents/ benefits fraud was the most common type of identity theft reported by consumers in 2015, comprising 49.2 percent of all identity theft complaints.[108]

For the first time in 15 years, however, identity theft was not the FTC's most common consumer complaint in 2015. Even so, 490,220 Americans still reported being victimized.[109] Consumers age 50 and older reported 45 percent of the identity theft complaints that the FTC received in 2015.[110]

The growing use of commercial tax filing software and online tax filing services has led to opportunities for thieves to commit fraud without stealing SSNs. In some cases, thieves can illegally access an existing customer's account simply by entering that individual's username, 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 long-standing policy and now will provide victims with copies of the fake returns upon written request.[111] The documents will provide victims with details to help them discover how much of their personal information was stolen. The IRS saw a marked improvement in the battle against identity theft in 2016.[112] According to the IRS, the number of people reporting stolen identities on federal tax returns fell by more than 50 percent, with nearly 275,000 fewer victims compared to a year ago.[113]

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.

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.[114] On October 7, 2015, the Aging Committee held a hearing titled, *"Protecting Seniors from Identity Theft: Is the Federal Government Doing Enough?"*[115] 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.[116]

Fraud Case #16

"Charles," from Maine, contacted the Fraud Hotline after learning that he was the victim of tax identity theft. When Charles tried to file his taxes online, the IRS notified him that someone had already submitted a tax return using his Social Security number (SSN). He says he was told that it could take up to six months for the issue to be resolved and for him to receive his tax return. A Fraud Hotline investigator worked with Charles and his local Taxpayer Advocate Service to process his return in six weeks. Once Charles received his refund, the Taxpayer Advocate advised him that the IRS would apply extra scrutiny to his return for the next three years to help ensure that no one tries to use his 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.

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/

Conclusion

One of the Senate Aging Committee's top priorities in the 115th Congress will be to continue combatting fraud that targets seniors. The Fraud Hotline has been instrumental in this fight, providing more than 2,280 callers in 2016 with information on common scams and offering tips on how to avoid becoming victims of fraud. In addition, Fraud Hotline investigators have encouraged victims to report fraud to the appropriate law enforcement agencies to improve the government's data as well as its ability to prosecute the perpetrators of these scams. Committee investigators have even helped some victims recover thousands of dollars of their hard-earned retirement savings.

The Aging Committee has held hearings on seven of the top ten scams on this list, with five of those hearings occurring in the last Congress. 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. The Committee has 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 the 115th Congress, Chairman Collins and Ranking Member Casey intend to maintain the Committee's focus on frauds targeting seniors and will continue to work with their Senate colleagues to ensure that law enforcement has the tools it needs to pursue these criminals and to encourage a more effective federal response to these scams.

This Fraud Book is designed to serve as a resource for seniors and others who wish to learn more about common scams and ways to avoid them. For further assistance, please do not hesitate to call the Aging Committee's Fraud Hotline at **1-855-303-9470**.

Appendix 1: Aging Fraud Hotline Statistics

Scam Type	Total
IRS Scam	1680
Sweepstakes Scam	124
Unsolicited Phone Calls	92
Computer Scam	77
Elder Abuse	53
Grandparent Scam	39
Romance Scam	36
Government Grant	35
Check Scam	23
Identity Theft	15
Utility Scams	14
Health-Related Scam	12
Social Security Fraud	9
Debt Collection Scam	8
Home Improvement Scam	8
Spam Email	8
Investment Fraud	7
Grand Jury Impersonation Scam	6
Legal Referral	7
Payday Lending	4
Timeshare Scam	4
IRS Fraudulent Tax Returns	3
Bad Business Practices	2
Bank Fraud	3
Charity Scam	2
DME Scam	2
Pension/Retirement Savings Fraud	2
SMishing Scam	2
Dietary Supplements	1
Free Trial Scam	1
Immigration Scam	1
Insurance Fraud	1
Kidnapping Scam	1

TOTAL	2282

Origin of Calls to the Hotline	Total
Alabama	38
Alaska	6
Arizona	29
Arkansas	5
California	145
Colorado	11
Connecticut	4
Delaware	5
District of Columbia	7
Florida	62
Georgia	14
Hawaii	3
Idaho	1
Illinois	22
Indiana	6
Iowa	3
Kansas	7
Kentucky	7
Louisiana	4
Maine	800
Maryland	143
Massachusetts	19
Michigan	33
Minnesota	17
Mississippi	3
Missouri	7
Montana	4

Origin of Calls to the Hotline	Total
Montana	1
Nebraska	6
Nevada	9
New Hampshire	7
New Jersey	28
New Mexico	9
New York	113
North Carolina	23
North Dakota	1
Ohio	35
Oklahoma	6
Oregon	10
Pennsylvania	96
Rhode Island	56
South Carolina	15
South Dakota	2
Tennessee	11
Texas	271
Unknown	7
Utah	44
Vermont	1
Virginia	32
Washington	79
West Virginia	6
Wisconsin	11
Wyoming	2

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
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	1800-366-4484
HHS OIG	http://www.hhs.gov/grants/grants/avoid-grant-scams/index.html	1-800-447-8477
National Center for Victims of Crime	https://www.victimsofcrime.org/	1-855-484-2846
FINRA Securities Helpline for Seniors	http://www.finra.org/investors/finra-securities-helpline-seniors	1- 844-574-3577
Center for Elder Rights Advocacy	http://www.legalHotlines.org/legal-assistance-resources.html	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	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
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 18, 2017.

[3] TIGTA Email to Aging Committee. January 21, 2017.

[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 22, 2017).

[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 . August 6, 2015. (accessed January 22, 2017).

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

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

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

[11] TIGTA. staff briefing with Senate Aging Committee staff on January 25, 2017.

[12] Ibid

[13] Ibid.

[14] Ibid.

[15] Department of Justice. Two Bristol Residents Arrested for Participating in IRS Impersonation Scam. September 15, 2016. https://www.justice.gov/usao-ct/pr/two-bristol-residents-arrested-participating-irs-impersonation-scam (accessed on January 25, 2017).

[16] Ibid.

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

[18] TIGTA Conference Call with Aging Committee. December 9, 2016.

[19] TIGTA Conference Call with Aging Committee. January 22, 2017.

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

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

[22] 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.

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

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

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

[26] U.S. Senate, 876-SCAM, S. 6-7.

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

[28] Federal Trade Commission. National Do Not Call Registry Data Book FY 2016. December 2016. https://www.ftc.gov/system/files/documents/reports/national-do-not-call-registry-data-book-fiscal-year-2016/dnc_data_book_fy_2016_post.pdf. Pg. 4. (accessed January 22, 2017).

[29] 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.

[30] Ibid.

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

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

[33] Ibid.

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

[35] Ibid.

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

17, 2015. (accessed January 22, 2017).

[37] Ibid.

[38] 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.

[39] Ibid.

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

[41] Federal Bureau of Investigation. Internet Crime Complaint Center. May 2016. *2015 Internet Crime Report*. (May 9): 12. https://pdf.ic3.gov/2015_IC3Report.pdf (accessed on January 22, 2017).

[42] Ibid., 13.

[43] Federal Trade Commission. February 2015. Consumer Sentinel Data Book: 82. https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2015/160229csn-2015databook.pdf. (accessed on January 22, 2017).

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

[45] Ibid., S. 18.

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

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

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

[49] 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).

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

[51] Ibid., 14.

[52] Ibid., 15.

[53] 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).

[54] 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.

[55] Ibid.

[56] Ibid., 10.

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

[58] 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).

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

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

[61] GAO, Elder Justice, 22.

[62] Ibid., 25-26

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

[64] 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).

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

[66] Ibid.

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

[68] Ibid.

[69] Ibid.

[70] Ibid.

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

[72] Ibid.

[73] Ibid.

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

[75] Federal Trade Commission. February 2015. *Consumer Sentinel Network Data Book*, 82.

[76] 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

[77] 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.

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

[79] Federal Trade Commission. Consumer Information: Online Dating Scams. http://www.consumer.ftc.gov/articles/0004-online-dating-scams (accessed January 22, 2017).

[80] 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 Febraury 14, 2013. (accessed January 22, 2017).

[81] FBI. 2015 Computer Crime Report, 15-16 https://pdf.ic3.gov/2015_IC3Report.pdf (accessed on January 22, 2017).

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

[83] Ibid.

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

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

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

[87] Ibid., 81.

[88] Ibid

[89] Federal Trade Commission. Fake Checks. https://www.consumer.ftc.gov/articles/0159-fake-checks#Youandyourbank (accessed on January 23, 2017).

[90] Ibid.

[91] American Bankers Association. Fake Check Scams. http://www.aba.com/Consumers/Pages/FakeCheckScams.aspx (accessed on January 23, 2017).

[92] Consumer Federation of America. Consumer Tips: Fake Check Scams. September 9, 2010. http://consumerfed.org/pdfs/Check_Scam_Web_Eng2.pdf (accessed on January 23, 2017).

[93] Federal Trade Commission. Fake Checks. https://www.consumer.ftc.gov/articles/0159-fake-checks#Youandyourbank (accessed on January 23, 2017).

[94] Ibid.

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

[96] Federal Trade Commission. Fake Checks. https://www.consumer.ftc.gov/articles/0159-fake-checks#Youandyourbank (accessed on January 23, 2017).

[97] Ibid.

[98] Ibid.

[99] Ibid.

[100] Department of Justice. Justice Department and Law Enforcement Partners Announce Civil and Criminal Actions to Dismantle Global Network of Mass Mailing Fraud Schemes Targeting Elderly and Vulnerable Victims. September 22, 2016. https://www.justice.gov/opa/pr/justice-department-and-law-enforcement-partners-announce-civil-and-criminal-actions-dismantle (accessed on January 23, 2017).

[101] Ellis, Blake and Melanie Hicken. Exposed: The Secrety powerhouse processing millions in global Fraud. CNN. September 22, 2016. http://money.cnn.com/2016/09/22/news/companies/pacnet-investigation/ (accessed on January 23, 2017).

[102] Department of Justice. Justice Department and Law Enforcement Partners Announce Civil and Criminal Actions to Dismantle Global Network of Mass Mailing Fraud Schemes Targeting Elderly and Vulnerable Victims. September 22, 2016. https://www.justice.gov/opa/pr/justice-department-and-law-enforcement-partners-announce-civil-and-criminal-actions-dismantle (accessed on January 23, 2017).

[103] Ibid.

[104] Ibid.

[105] United States District Court Eastern Districk of New York. Criminal Complaint: 4. September 4, 2016. https://www.justice.gov/opa/file/895141/download. (accessed on January 23, 2017).

[106] Department of Justice. Justice Department and Law Enforcement Partners Announce Civil and Criminal Actions to Dismantle Global Network of Mass Mailing Fraud Schemes Targeting Elderly and Vulnerable Victims. September 22, 2016. https://www.justice.gov/opa/pr/justice-department-and-law-enforcement-partners-announce-civil-and-criminal-actions-dismantle (accessed on January 23, 2017).

[107] Ibid.

[108] Ibid., 12.

[109] FTC, 2015 *Consumer Sentinel Network Data Book*, 6. https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2015/160229csn-2015databook.pdf (accessed on January 22, 2017).

[110] Ibid, 14

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

[112] IRS. As Holidays Approach, IRS Reminds Taxpayers of Refund Delays in 2017. November 22, 2016. https://www.irs.gov/uac/as-holidays-approach-irs-reminds-taxpayers-of-refund-delays-in-2017 (accessed on January 22, 2017).

[113] Ibid.

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

[115] 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.

[116] Ibid., S. 12-15 and S.17-20.

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

1-855-303-9470