113TH CONGRESS
2d Session

SENATE

REPORT
113–305

FIGHTING FRAUD: LESSONS LEARNED FROM THE SENATE AGING COMMITTEE'S CONSUMER HOTLINE

R E P O R T

OF THE

SPECIAL COMMITTEE ON AGING
UNITED STATES SENATE

DECEMBER 11, 2014.—Ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE

49–010 WASHINGTON : 2014

SPECIAL COMMITTEE ON AGING

BILL NELSON, Florida, *Chairman*

BOB CASEY, Pennsylvania
CLAIRE MCCASKILL, Missouri
SHELDON WHITEHOUSE, Rhode Island
KIRSTEN GILLIBRAND, New York
JOE MANCHIN, West Virginia
RICHARD BLUMENTHAL, Connecticut
TAMMY BALDWIN, Wisconsin
JOE DONNELLY, Indiana
ELIZABETH WARREN, Massachusetts
JOHN WALSH, Montana

SUSAN COLLINS, Maine
Ranking Member
BOB CORKER, Tennessee
ORRIN HATCH, Utah
MARK KIRK, Illinois
DEAN HELLER, Nevada
JEFF FLAKE, Arizona
KELLY AYOTTE, New Hampshire
TIM SCOTT, South Carolina
TED CRUZ, Texas

KIM LIPSKY, *Staff Director*
PRISCILLA HANLEY, *Staff Director*

LETTER OF TRANSMITTAL

U.S. SENATE,
SPECIAL COMMITTEE ON AGING,
Washington, DC, December 11, 2014.

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

DEAR MR. PRESIDENT: Under the authority of Senate Resolution 253, agreed to on October 3, 2013, I am submitting to you a report of the U.S. Senate Special Committee on Aging entitled: Fighting Fraud: Lessons Learned from the Senate Aging Committee's Consumer Hotline.

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

I am pleased to transmit this report to you.

Sincerely,

BILL NELSON, *Chairman.*

CONTENTS

113TH CONGRESS
2d Session

SENATE

REPORT
113–305

FIGHTING FRAUD: LESSONS LEARNED FROM THE SENATE AGING COMMITTEE'S CONSUMER HOTLINE

DECEMBER 11, 2014.—Ordered to be printed

Mr. NELSON, from the Special Committee on Aging, submitted the following

R E P O R T

EXECUTIVE SUMMARY

Recognizing the epidemic of fraud perpetrated against seniors in the United States, and the extent to which the victims of fraud are often unsure of where they should turn for help, the United States Senate Special Committee on Aging launched a Fraud Hotline in November 2013. In the Hotline's first year, Committee staff has responded to more than 1,900 reports of fraud impacting seniors. Categories of fraud commonly reported to the Hotline included phone scams, such as international lottery scams and impostor scams, identity theft, Social Security fraud and tax-related fraud. Every day, the Hotline not only shares valuable information with older Americans and their loved ones who reach out for assistance, but it also provides crucial information to the Committee by offering a real-time glimpse into the nature and variety of scams targeting seniors—information the Committee has used to better focus its investigations, hearings and efforts to educate and protect older consumers.

I. INTRODUCTION

In the 113th Congress, the U.S. Senate Special Committee on Aging has pursued an aggressive agenda aimed at protecting older Americans from fraudulent and deceptive practices. As Chairman and Ranking Member of the Committee, Senators Bill Nelson and Susan Collins have held hearings to examine a variety of scams often targeted at seniors. At the beginning of 2013, the Committee focused its attention on the Jamaican lottery scam, a widespread scheme in which fraudsters lead victims to believe they have won a lottery but must pay upfront fees or taxes before their winnings

can be released.[1] The following month, the Committee held a hearing to explore ways to combat tax-related identity theft,[2] a crime that grew rapidly from 2008 to 2012, according to the Internal Revenue Service Taxpayer Advocate Service.[3] The Committee then held a hearing to spotlight the targeting of Social Security benefits by identity thieves in which it examined steps the Social Security Administration (SSA) and the Department of Treasury were taking to combat this fraud.[4]

In March of 2014, the Committee examined fraud in the Medicare program and ways in which fraud prevention measures might be strengthened to protect seniors and taxpayers.[5] The following month, the Committee released the findings of a year-long Committee staff investigation into unscrupulous precious metals firms and held a hearing to explore its findings.[6] Also in April of 2014, the Committee released an investigative report that detailed potentially widespread deception in the promotion of sweepstakes popular among seniors.[7]

In July of this year, the Committee revisited the scourge of phone scams, with particular emphasis on the grandparent scam—in which a con artist impersonates a family member or friend—and heard testimony from the Federal Bureau of Investigations (FBI) and Federal Trade Commission (FTC) about their efforts to track down the fraudsters.[8] Most recently, the Committee examined the role of the private sector in stemming the tide of phone scams.[9]

As the Committee has examined this array of scams in its investigations and hearings, two issues that have arisen repeatedly include the frequency with which victims do not report fraud and the difficulty they encounter in determining where they should turn when they wish to report a scam to law enforcement. These concerns are not new, but rather, they are well documented. For example, an AARP study found that 75 percent of victims age 55 and over did not report the fraud.[10] A study by the National White Col-

---

[1] U.S. Senate Special Committee on Aging, *876-SCAM: Jamaican Phone Fraud Targeting Seniors* (March 13, 2013) (online at http://www.aging.senate.gov/hearings/hearing-876-scam-jamaican-phone-fraud-targeting-seniors)

[2] U.S. Senate Special Committee on Aging, *Tax-Related Identity Theft: An Epidemic Facing Seniors and Taxpayers* (April 10, 2013) (online at http://www.aging.senate.gov/hearings/tax-related-identity-theft-an-epidemic-facing-seniors-and-taxpayers)

[3] Taxpayer Advocate Service, *2012 Annual Report to Congress* (Dec. 31, 2012) (online at http://www.taxpayeradvocate.irs.gov/userfiles/file/2012-Annual-Report-to-Congress-Executive-Summary.pdf)

[4] U.S. Senate Special Committee on Aging, *Social Security Payments go Paperless: Protecting Seniors from Fraud and Confusion* (June 19, 2013) (online at http://www.aging.serate.gov/hearings/social-security-payments-go-paperless-protecting-seniors-from-fraud-and-confusion)

[5] U.S. Senate Special Committee on Aging, *Preventing Medicare Fraud: How Can We Best Protect Seniors and Taxpayers?* (March 26, 2014) (online at http://www.aging.senate.gov/hearings/preventing-medicare-fraud-how-can-we-best-protect-seniors-and-taxpayers)

[6] U.S. Senate Special Committee on Aging, *Exploring the Perils of the Precious Metals Market* (April 30, 2014) (online at http://www.aging.senate.gov/hearings/exploring-the-perils-of-the-precious-metals-market)

[7] U.S. Senate Special Committee on Aging, *Pushing the Envelope: Publishers Clearing House in the New Era of Direct Marketing*, Senate Report 113–153 (April 11, 2014) (online at: http://www.aging.senate.gov/imo/media/doc/PCH_REPORT_4_20141.pdf)

[8] U.S. Senate Special Committee on Aging, *Hanging Up on Phone Scams: Progress and Potential Solutions to this Scourge* (July 16, 2014) (online at http://www.aging.senate.gov/hearings/-hanging-up-on-phone-scams-progress-and-potential-solutions-to-this-scourge)

[9] U.S. Senate Special Committee on Aging, *Private Industry's Role in Stemming the Tide of Phone Scams* (Nov. 19, 2014) (online at http://www.aging.senate.gov/hearings/private-industrys-role-in-stemming-the-tide-of-phone-scams)

[10] AARP, *AARP Foundation National Fraud Victim Study* (March 2011) (online at http://assets.aarp.org/rgcenter/econ/fraud-victims-11.pdf)

lar Crime Center found that, even when victims did report a scam, only 12 percent reported to a criminal justice entity.[11]

In the context of these concerns, the Committee launched its Fraud Hotline, an innovative resource to which individuals can report instances of fraud or scams affecting seniors. The Hotline is consistently staffed during business hours with investigators who have experience with investment scams, identity theft, bogus sweepstakes and lottery schemes, Medicare and Social Security fraud and a variety of other scams of which seniors are often the victims.

The Hotline seeks to assist individual consumers by providing callers with personalized advice regarding steps that can be taken when a senior is the target of a scam, including where to report the fraud and ways to reduce the likelihood that the senior becomes a victim or repeat victim. Seniors are typically referred by investigators to the local, state and/or federal law enforcement entities with jurisdiction over the particular scam. In addition to law enforcement, Committee staff may also direct seniors to other resources, such as consumer protection groups, legal aid clinics, Congressional caseworkers or local nonprofits that provide aid to seniors.

When appropriate, seniors are also provided with steps they can take to reduce the likelihood that they become victims or repeat victims. For example, when a senior reports an instance of identity theft, he may be advised to place a fraud alert on his credit report with a major, national credit bureau; order free credit reports to ensure that he is aware of all attempts to fraudulently open accounts using his identity; contact his bank, credit card company or any other financial institution; and create an identity theft affidavit by reporting the theft to the FTC and filing a police report.[12] The victim should also report it to the Internal Revenue Service (IRS), who will flag his account and take precautions against someone fraudulently filing a tax return.

Meanwhile, the Hotline allows the Committee to keep a detailed and current record of common fraud schemes impacting seniors, which informs the efforts of the Committee, and ultimately the work of the U.S. Congress. With the goal of protecting the hard-earned life savings of older Americans, the Committee has used information gained through the Hotline to inform its investigations, hearings and efforts to educate older consumers—and to bring greater awareness to the epidemic of fraud perpetrated against our nation's seniors.

The resources offered by the Hotline were highlighted in numerous news articles across the country, including the January/February 2014 AARP Bulletin, which described the Hotline as a new effort aimed at shrinking the estimated $2.9 billion that older Americans lose to fraud each year.[13] Additionally, the *New York Times* featured the Hotline in a November 2013 article that explained that the resource "will give harried seniors and family members another place to turn besides local law enforcement, the

---

[11] National White Collar Crime Center, *The 2010 National Public Survey on White Collar Crime* (Dec. 2010) (online at http://www.nw3c.org/docs/publications/2010-national-public-survey-on-white-collar-crime.pdf?sfvrsn=8)

[12] Federal Trade Commission, Immediate Steps to Repair Identity Theft (August 2012) (online at http://www.consumer.ftc.gov/articles/0274-immediate-steps-repair-identity-theft)

[13] Steve Mencher, *Taking a Bite Out of Fraud*, AARP Bulletin (Jan.–Feb. 2014), p. 6.

Federal Trade Commission and adult protective services agencies."[14] The Hotline was also featured in various local publications.[15] Since its November 2013 launch, the Hotline has already responded to more than 1,900 individuals over the phone or through its online form.

This report serves as an overview of scams reported to the Hotline. The most common fraud schemes are highlighted, with a description of the scam and real-life stories of victims from across the country. Victims' names have been changed to protect their confidentiality and prevent the possibility of revictimization. It should be noted that some victims' experiences overlap into multiple categories of scams. For example, once an individual becomes the victim of identity theft, his information may also be used to commit fraud by redirecting his Social Security payment or by claiming his tax refund.

The most common scams reported to the Hotline include:

- Computer scams;
- Grandparent scams;
- Health-related scams, especially medical alert device scams;
- Identity theft, including reports of tax-related identity theft;
- Lottery scams, including reports of the Jamaican lottery scam;
- Social Security fraud;
- Timeshare scams; and

In addition to these categories, the Hotline has received more than 800 miscellaneous consumer complaints, which include many reports of deceptive business practices. The Hotline has also received a number of reports regarding guardianship issues, which typically involve financial abuse of a senior.

II. COMPUTER SCAMS

Increasingly, fraudsters have utilized computers to acquire personal information from victims. They often target seniors, who may be less technologically savvy than younger consumers. In a common variation of the scam, often referred to as a "tech support" scam, fraudsters gain the victim's trust by pretending to be from a well-known technology company, such as Microsoft, Dell or McAfee, claiming they can stop an impending computer hack or virus. In a typical variation of the scam, the fraudster will direct the senior to a screen on his computer that displays an activity log of the system, which the scammer will claim shows that the computer has been compromised. In reality, what is displayed on this screen is normal and does not indicate that there is any problem. Preying on the senior's fear, the scammers will then insist upon gaining re-

[14] Paula Span, *A New Way to Report Fraud*, New York Times (Nov. 26, 2013) (online at http://newoldage.blogs.nytimes.com/2013/11/26/a-new-way-to-report-fraud/?_php=true&_type=blogs&_r=0)

[15] *See, e.g.*, Sheryl Harris, *Senate Aging Committee Creates Fraud Hotline for Seniors: Plain Dealing*, cleveland.com (Nov. 19, 2013) (online at http://www.cleveland.com/consumeraffairs/index.ssf/2013/11/senate_aging_committee_creates.html); *Senate Aging Committee Launches Anti-Fraud Hotline: 1–855–303–9470*, St. John Valley Times (Nov. 13, 2013) (online at http://www.sjvalley-times.com/view/full_story/24048871/article-Senate-Aging-Committee-launches-anti-fraud-hotline—1–855–303–9470); and Alejandra Matos, *Senate Launches Anti-Fraud Hotline for Seniors*, Star Tribune (Jan. 20, 2014) (online at http://www.startribune.com/local/blogs/241188101.html)

mote access to a computer in order to fix the so-called emergency. Once they have gained access to the device, hackers will change the computer's settings to increase the computer's vulnerability, enroll the victim in worthless computer warranty programs, request credit card information to bill for supposed computer protection services, install malware to steal sensitive data or personal information and/or direct a victim to a fraudulent website to purchase software with a credit card.[16]

In October 2012, the FTC announced an international crackdown on tech support scammers, charging six operations, mostly based in India, with contacting consumers over the phone and pretending to be from legitimate computer companies.[17] The scammers tricked consumers into believing their computers were riddled with malware and then charged them to "fix" the problems. According to the FTC, the companies utilized 80 different domain names and 130 different phone numbers. Earlier this year, a U.S. District Court ordered the scam operators to pay more than $5.1 million.[18]

Depending on the extent of a computer scam victim's experience, investigators may direct the victim to several resources, including:

- The Internet Crime Complaint Center, also known as IC3, which is a partnership between the FBI and the National White Collar Crime Center.[19] The IC3 receives Internet-related complaints and refers them to federal, state, local or international law enforcement and/or regulatory agencies for whatever investigation they deem to be appropriate. The IC3 also provides information on current Internet schemes. In its 2013 annual report, the IC3 noted that the total combined losses for individuals over the age of 60 from reported Internet-related scams in 2013 were $160,129,686;[20] and
- The FTC, which is a beneficial resource for victims who would like more information on current Internet scams. The FTC also manages a scam email account for those who would like to report phishing emails.[21]

The Hotline has received a number of reports of computer scams, including the following stories:

- Margaret, a Florida resident, called the Hotline with concern about her husband, who was the victim of a computer scam. A fraudster, who claimed he was calling on behalf of Microsoft, contacted Margaret's husband and convinced him to send $400 via Western Union money transfer to pay for virus protections services. Margaret requested that an investigator speak to her husband to give him information about the prevalence of these scams and advice on how he might protect himself in the future. Like many seniors who contact the Hotline, Margaret's husband was very embarrassed about what had occurred. An investigator spoke with

---

[16] FTC, *Consumer Information: Tech Support Scams* (Jan. 2014) (online at http://www.consumer.ftc.gov/articles/0346-tech-support-scams)

[17] FTC, *FTC Halts Massive Tech Support Scams* (Oct. 3, 2012) (online at http://www.ftc.gov/news-events/press-releases/2012/10/ftc-halts-massive-tech-support-scams)

[18] FTC, Federal Court Orders Tech Support Scammers to Pay More Than $5.1 Million (July 24, 2014) (online at http://www.ftc.gov/news-events/press-releases/2014/07/federal-court-orders-tech-support-scammers-pay-more-51-million)

[19] The Internet Crime Complaint Center, *About IC3* (online at http://www.ic3.gov/about/default.aspx)

[20] The Internet Crime Complaint Center, *2013 Internet Crime Report* (May 2014) (online at http://www.nw3c.org/docs/IC3-Annual-Reports/2013-ic3-internet-crime-report.pdf?sfvrsn=4)

[21] FTC, *Consumer Information: Phishing* (Sept. 2011) (online at http://www.consumer.ftc.gov/articles/0003-phishing)

Margaret's husband and explained the prevalence of this scam and ways he might protect himself in the future. She was also encouraged to report the scams to the FTC.

• Steven, from Boston, Massachusetts, received a phone call from a scammer posing as a representative from Microsoft. The scammer claimed Steven's computer needed maintenance. The scammer was able to gain remote access to his computer and showed Steven a list of files that supposedly needed to be removed. Steven provided the scammer with his debit card information to pay for $10 service fee. Later, Steven realized that he had actually been charged $800. He contacted his bank to report the scam, but he was informed that the bank would be unable to recover his money. He is still receiving phone calls from fraudulent computer companies claiming he needs additional maintenance on his computer. An investigator encouraged Steven to report the scam to the FTC. The investigator also explained that Steven could contact his phone service provider to inquire about blocking some of the numbers from which he is still receiving the harassing calls.

• Bill from New York was scammed out of $750 after he received a phone call from someone claiming he had a virus on his computer that needed to be removed. After gaining remote access to his computer, the scammer convinced him to send a check to an address in Arizona. Bill did not realize that he was the victim of a scam until after the check had been cashed, and he has been unable to recover any of the money. Bill had already reported the scam to the New York Attorney General's office, which was looking into the matter, but he wanted to also make the Committee aware of this scam.

III. GRANDPARENT SCAMS

The Committee has received an alarming number of reports of scammers posing as a family member in need of help. Scammers claim they are with a family member, often a grandchild, who is in urgent need of money to cover medical care or fix a legal problem, such as money for bail or legal services after a supposed arrest. Scammers may obtain personal family information from social networking sites, which they use to make their stories more convincing.[22] In many cases, scammers will ask a victim to send money via a wire transfer service or purchase a prepaid debit product, such as the Green Dot MoneyPak.[23] The FTC categorizes grandparent scams as a subset of scams known as impostor scams. Impostor scams were the fourth most prevalent scam in 2013, with a total of 121,720 incidents reported to the FTC.[24]

The Committee held a hearing on July 16, 2014, to examine the role of the federal government, especially the FTC and FBI, in combating phone scams, with particular attention paid to the grandparent scam.[25] An Ohio grandfather explained how he lost $7,000

[22] Federal Bureau of Investigations, *The Grandparent Scam: Don't Let it Happen to You* (April 2, 2012) (online at http://www.fbi.gov/news/stories/2012/april/grandparent_040212)

[23] Green Dot, *About MoneyPak* (online at https://www.moneypak.com/AboutMoneyPak.aspx)

[24] FTC, *Consumer Sentinel Network Data Book for January–December 2013* (Feb. 2014) (online at http://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2013/sentinel-cy2013.pdf)

[25] U.S. Senate Special Committee on Aging, *Hanging Up on Phone Scams: Progress and Potential Solutions to this Scourge* (July 16, 2014) (online at http://www.aging.senate.gov/hearings/-hanging-up-on-phone-scams-progress-and-potential-solutions-to-this-scourge)

after he received a call from someone impersonating his grandson and claiming he had been arrested and needed bail money immediately.[26] The victim transferred money to the fraudsters using Green Dot MoneyPaks, which are PIN-based reload cards that allow a scammer to remotely receive payment from a victim in a manner that is very difficult to trace. Last year, Americans reported losing $42.86 million to schemes involving prepaid products.[27] The MoneyPak is the prepaid reload card of choice for many scammers and a product the Committee has examined closely, along with two corresponding products: InComm's Vanilla Reload[28] and Blackhawk Network's Reloadit Pack.[29] During the hearing, Chairman Nelson announced that Green Dot would be discontinuing their MoneyPak product in the coming months.[30] Additionally, InComm recently announced that it would also be pulling its Vanilla Reload in the first quarter of 2015, and Blackhawk shared with the Committee its plans to introduce enhanced security features.[31]

Resources to which victims of grandparent scams are referred include:

- State Attorneys General;
- State consumer protection agencies;
- Local law enforcement authorities;
- The Department of Homeland Security's Immigration and Customs Enforcement (ICE) tip line; and
- The FTC.

Committee staff continues to explore what can be done to help seniors defend against fraudulent calls before they pick up the phone.

Grandparent scam victims have reported the following stories through the Hotline:

• Mary, who lives in Illinois, received a phone call from a scammer posing as her grandson. He claimed he was on vacation in the Dominican Republic and was calling because he had been arrested for drug possession. He pleaded that she keep the arrest a secret from his parents until he was safe. The scammer sounded just like her grandson and gave Mary specific directives on what she should say at the bank in order to withdraw a significant amount of money without raising suspicions. The scam continued to evolve, and he later asked for money for a lawyer. In the end, Mary lost over $25,000. She had already reported the scam to local, state and federal law enforcement, but she had been unable to recover any money. She contacted the Hotline to share her story so

---

[26] Cincinnati.com, *Local Testifies About 'Grandparent Scam' Before Senate* (July 16, 2014) (online at http://www.cincinnati.com/story/news/crime/2014/07/16/cincinnati-man-grandparent-scam-senate/12762055/)

[27] Matthew Goldstein, *MoneyPak, a Popular Prepaid Money Card, Opens Path to Fraud Schemes* (July 31, 2014) (online at http://dealbook.nytimes.com/2014/07/31/popular-prepaid-money-card-opens-path-to-fraud-schemes/?_php=true&_type=blogs&_r=0)

[28] *See* Vanilla Reload, *How Reload Works* (online at https://www.vanillareload.com/howitworks)

[29] *See* Reloadit, *How it Works* (online at https://www.reloadit.com/HowItWorks)

[30] U.S. Senate Special Committee on Aging, *Hanging Up on Phone Scams: Progress and Potential Solutions to this Scourge,* Opening Statement of Chairman Nelson (July 16, 2014) (online at http://www.aging.senate.gov/imo/media/doc/Nelson_7_16_14.pdf)

[31] U.S. Senate Special Committee on Aging, *Private Industry's Role in Stemming the Tide of Phone Scams,* Testimony of Skeet Rolling and William Y. Tauscher (Nov. 19, 2014) (online at http://www.aging.senate.gov/hearings/private-industrys-role-in-stemming-the-tide-of-phone-scams)

that others could be educated and avoid the difficulty she had experienced.

• Emily in Louisiana received a phone call from a scammer who she believed was her son. The scammer said he was in jail in Mexico City and asked Emily to contact a bail bondsman as soon as possible. Emily sent the scammers $20,000. The next day, Emily received a phone call from her son, who was at home in California. He informed her that he was never in Mexico City. Emily contacted the Hotline in search of guidance on what law enforcement entities might be able to investigate this crime. An investigator provided Emily with the contact information for the ICE tip line, the FTC and her state Attorney General to report the scam for further investigation.

• Mark's grandmother, a resident of California, was contacted by an individual claiming to be from the United States Embassy in Mexico. He alleged that Mark had been arrested on drug charges. The scam went on for over a month and Mark's grandmother sent the scammers more than $70,000, costing her nearly all of her life savings. Mark contacted the Hotline to share his grandmother's story, hoping it could be used to educate other seniors and prevent future scams. The Committee was ultimately able to connect Mark with a journalist who was interested in writing about his grandmother's story to warn unsuspecting seniors of this scam.

• Robert, a California resident, received a call from a scammer posing as his oldest grandson. He claimed he had been in an accident and was in a hospital in Mexico. He asked Robert for money to pay his hospital bill, which he said he had to do before he would be allowed to leave the country. Robert sent money, but he soon found out he was the victim of a scam. He contacted the Hotline to inquire about whether he might have any recourse. An investigator provided Robert with the contact information for the FTC, the ICE tip line and his state's Attorney General.

IV. HEALTH-RELATED SCAMS

The Committee has sought to address the significant challenge of Medicare fraud with consistent oversight of the Department of Health & Human Services' (HHS) fraud prevention efforts targeted at Medicare payments.[32] Although estimating how much money is lost each year to Medicare fraud presents various challenges, there is no doubt the number is staggering, with one estimate of $60–$90 billion.[33]

In March 2014, the Committee held a hearing titled: "Preventing Medicare Fraud: How Can We Best Protect Seniors and Taxpayers?"[34] The hearing highlighted expanded authority granted by the Affordable Care Act to the Centers for Medicare and Medicaid Services (CMS) to use in its fight against fraud. The cost of Medi-

[32] Department of Health and Human Services, Center for Medicare & Medicaid Services, *Medicare Fraud & Abuse—Prevention, Detection, and Reporting* (Aug. 2014) (online at http://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/downloads/Fraud_and_Abuse.pdf)

[33] Merrill Matthews, *Medicare and Medicaid Fraud is Costing Taxpayers Billions* (May 2012) (online at http://www.forbes.com/sites/merrillmatthews/2012/05/31/medicare-and-medicaid-fraud-is-costing-taxpayers-billions/2/)

[34] U.S. Senate Special Committee on Aging, *Preventing Medicare Fraud: How Can We Best Protect Seniors and Taxpayers?* (March 26, 2014) (online at http://www.aging.senate.gov/hearings/preventing-medicare-fraud-how-can-we-best-protect-seniors-and-taxpayers)

care fraud, however, is not limited to the number of dollars lost, and the Hotline is a reminder of the toll Medicare fraud can take on the life of a vulnerable senior.

The majority of health-related scams reported to the Hotline involve seniors receiving fraudulent calls about medical alert devices. A medical alert device is an electronic device, typically worn on a bracelet or necklace, which is used to alert responders of an emergency situation. Medical alert device scammers attempt to collect personal information or convince a senior to pay for a device or service he never ordered.[35] If collected, personal information will likely be used in identity theft schemes, such as opening lines of credit in a victim's name or redirecting a victim's Social Security benefits.

A typical medical alert device scam begins with an automated phone call informing the target that someone, usually a family member or friend, has ordered a medical alert device for the senior. The recording explains that the device has already been paid for, and sometimes free groceries are offered as an added incentive. A phone menu gives the target the option of opting out—which likely only confirms that the phone number is active—or speaking to a representative about confirming delivery. If the target chooses the latter, the representative will tell the victim that, although the device has already been paid for, he must provide payment for monthly or annual operating fees. This fee may be as much as $35 a month.[36] The scammer may also claim that personal information is needed to confirm delivery.

The medical alert device scammers should not be confused with companies that legitimately provide real services. Unlike scammers pretending to offer a service as a way to gain personal information and payment, legitimate companies provide real equipment and services, and they charge only for systems customers have actually ordered. Legitimate companies are usually registered with organizations like the Better Business Bureau and do not solicit through an automated phone call.

Depending on the category of scam reported, investigators may direct victims to a variety of resources; for example:

- Callers wishing to report suspected cases of Medicare fraud, waste or abuse may be referred to the HHS Office of the Inspector General (OIG), which accepts tips and complaints about potential fraud, waste, abuse and mismanagement in the agency's programs.
- If a caller has questions or concerns regarding billing, and the investigator is unable to assist him, he may be encouraged to contact CMS or the Medicare Rights Center.[37]
- Callers reporting medical alert device scams may be referred to their state Attorneys General, the FTC and the Federal Communications Commission (FCC).

Health-related scam victims include:

---

[35] Sid Kirchheimer, *'Free' Medical Alert Device Offers Harm, Not Help*, AARP Bulletin (July 2013) (online at http://www.aarp.org/money/scams-fraud/info-07-2013/free-medical-alert-device-offers-hurt-more-than-help.html)

[36] Gitte Laasby, *Robocalls Targeted Elderly, Shut-Ins*, Milwaukee Journal Sentinel (Jan. 2014) (online at http://www.jsonline.com/watchdog/pi/judge-halts-suspected-medical-alert-device-scam-b99182956z1-239947171.html)

[37] The Medicare Rights Center is a national nonprofit consumer organization that provides information on Medicare rights and benefits.

• Edward, a resident of Massachusetts, received a phone call from a health company claiming he was eligible for two knee braces under Medicare. This company had information about his Medicare, causing Edward to believe it was legitimate. Once the two knee braces arrived, they were not what Edward was told he was ordering and he is unable to use them. Medicare was charged $1,700. Edward is in desperate need of knee braces, but he will not be eligible to receive another pair for five years. Edward was referred by an investigator to the OIG and his State Health Insurance Assistance Program for further assistance.

• Tom received phone calls from a company that claimed it was contacting him to arrange the delivery of the medical alert system he had ordered, even though he never ordered any such system. When this company called, his phone displayed "Alert" in the Caller ID field, which piqued his curiosity and led him to answer the phone. Fortunately, Tom was aware that these calls were part of a scam. Committee staff recommended that Tom register for the National Do-Not-Call Registry and then file complaints about any unsolicited calls. Tom was also advised to contact the FTC.

• Sarah, a senior living in Colorado, received phone calls claiming a family member purchased a medical alert device for her. She received as many as 10 calls in a single day. It is difficult for Sarah to get to the phone, and she does not have Caller ID to screen these fraudulent calls. Sarah is in a constant state of frustration because she cannot stop the calls. An investigator encouraged Sarah to simply not answer these calls—as answering the calls will often only lead to more calls—and provided her with the contact information for the FTC.

V. IDENTITY THEFT

Identity theft occurs when a fraudster uses someone's personal information without permission. Thieves access personal information through numerous means, including stealing a wallet, purse, or mail; posing as a legitimate company and requesting information in a phone or email scam; sifting through the trash; accessing information provided to an unsecured Internet site; and obtaining credit reports by posing as a landlord or employer.[38] [39] The FTC has reported identity theft as the number one consumer complaint for 14 years in a row.[40] Additionally, of the total number of identity theft complaints in 2013, the FTC reported that 20 percent came from victims age 60 and older.[41]

Medical identity theft can occur when scammers pose as representatives of Medicare. If successful, the scammer will obtain a person's Social Security number or Medicare number and use it to receive medical care, purchase drugs or submit fake billings to Medicare in the victim's name.[42] Among other tricks, scammers

[38] IRS, *Identity Protection Tips* (October 2014) (online at http://www.irs.gov/uac/Identity-Protection-Tips)

[39] U.S. Department of Education Office of Inspector General, *How Identity Theft Happens* (July 2009) (online at http://www2.ed.gov/about/offices/list/oig/misused/how.html)

[40] Ben Popken, *ID Theft Tops FTC's Consumer Complaint List*, Today (Feb. 27, 2014) (online at http://www.nbcnews.com/business/consumer/id-theft-tops-ftcs-consumer-complaint-list-n40356)

[41] FTC, *Consumer Sentinel Network Data Book for January–December 2013* (Feb. 2014) (online at http://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2013/sentinel-cy2013.pdf)

[42] Stopmedicarefraud.gov, *Medical Identity Theft & Medicare Fraud*, U.S. Department of Health and Human Services, HHS Office of the Inspector General, Center for Medicare and

often ask the target to confirm certain personal information in order to supposedly receive information on Medicare services for which he is eligible. It is important to note that representatives of Medicare will never come to an individual's home uninvited to sell products. Also, representatives of Medicare are not allowed to ask for a person's Social Security number, bank account information or Medicare number over the phone.[43]

Tax-related identity theft is a growing variation of identity theft. Based on complaints reported to the FTC's Consumer Sentinel Network during 2013, around 30 percent of identity theft complaints involved tax-related identity theft.[44] A September 2014 Government Accountability Office (GAO) report found that in the 2013 filing season, the IRS paid out $5.2 billion to fraudsters, an increase of $1.6 billion from what the agency's inspector general identified in the 2012 tax-filing season.[45]

The Committee held a hearing in April 2013 titled: "Tax-Related Identity Theft: An Epidemic Facing Seniors and Taxpayers."[46] The hearing examined how fraudsters carry out their tax-related identity theft schemes and what taxpayers can do to protect their personal information. A victim of tax-related identity theft, Marcy Hossli, shared her story with the Committee. After receiving a letter from the IRS informing her she was the victim of tax fraud, Ms. Hossli spent three years trying to fix what had occurred. She reached out to several federal agencies to assist her, but she received no significant assistance. Chairman Nelson's office was the first resource she contacted that actually helped to fix her problem.

Based on information provided by victims, investigators may:

- Encourage a victim to file a report with his local police department, which can be used to prove that he has been a victim of identity theft;
- Advise a victim to establish a fraud alert with the national credit bureaus;
- Direct a victim to the FTC to file an identity theft affidavit. The FTC will also provide the victim with information to better understand the process of repairing his identity and prevent against further compromises;
- If the victim is a target of tax fraud, he will be encouraged to contact the IRS's Identity Protection Specialized Unit or his local taxpayer advocate; and
- If a Social Security number was obtained by a fraudster, the victim will be provided with the contact information for the SSA to report the theft of a Social Security number.

Of the many reports of identity theft received by the Hotline, the following victims paid a significant price:

Medicaid Services, and U.S. Department of Justice (online at http://www. stopmedicarefraud.gov/toolkit/documents/fightback_brochure_rev.pdf)

[43] Center for Medicare & Medicaid Services, *Protect Medicare and You from Fraud* (Aug. 2014) (online at http://www.medicare.gov/pubs/pdf/10111.pdf)

[44] FTC, *FTC Announces Top National Consumer Complaints for 2013* (Feb. 2014) (online at http://www.ftc.gov/news-events/press-releases/2014/02/ftc-announces-top-national-consumer-complaints-2013)

[45] Government Accountability Office, *Identity Theft: Additional Actions Could Help IRS Combat the Large, Evolving Threat of Refund Fraud* (Aug. 2014) (online at http://www.gao.gov/assets/670/665368.pdf)

[46] U.S. Senate Special Committee on Aging, *Tax-Related Identity Theft: An Epidemic Facing Seniors and Taxpayers* (April 10, 2013) (online at http://www.aging.senate.gov/hearings/tax-related-identity-theft-an-epidemic-facing-seniors-and-taxpayers)

• Martha's wallet was stolen and the perpetrator began using her information to accumulate $13,000 of debt in Martha's name. Although she has filed a report with her credit card company and local police department, she has been unsuccessful in her attempts to remove this debt from her credit report. Martha contacted the Hotline for help in her dealings with the credit bureaus and assistance with how she might protect herself from a future compromise of her personal information. An investigator provided Martha with basic steps she could take to protect her personal information and directed her to the FTC for additional information on identity theft. The investigator also referred her to the Consumer Financial Protection Bureau and explained how it might be able to help her in her dispute with the credit bureaus.

• Mindy's mother, who lives in Missouri, was visited by a door-to-door salesman who claimed she could sign up for a service that would bring a doctor to her home to explain what Medicare services she was eligible to receive. Mindy's mother signed the forms, which asked for her Social Security number and Medicare number. Mindy contacted the Hotline to receive assistance in preventing her mother from becoming the victim of identity theft. Mindy was referred to the SSA to report the theft of her mother's Social Security number and Medicare number. An investigator further encouraged Mindy to contact the national credit bureaus and the FTC to file an identity theft affidavit.

• Julie has been a victim of identity theft since 2007, when someone began using her name and Social Security number to apply for credit cards and loans. In 2011, a fraudulent IRS tax return was submitted using her name, home address and Social Security number. Julie contacted the Hotline looking for help with this matter with which she has struggled for years. An investigator referred Julie to the FTC to report the fraud and to file an identity theft affidavit. She was further referred to the SSA to report the fraudulent use of her Social Security number. She was also referred to the IRS's Identity Protection Specialized Unit.

VI. LOTTERY SCAMS

An especially prevalent scam often targeted at unsuspecting seniors involves telephone calls and direct mail, usually originating overseas, that claim the targets have won a lottery. Scammers explain that victims must make an advanced payment to cover taxes or fees in order to claim their winnings. Scammers typically request payment via wire transfer, such as MoneyGram or Western Union, or ask the victim to purchase a prepaid debit reload card, such as the Green Dot MoneyPak.

Over time, the scammer's story evolves, with various excuses as to why the winnings have not been delivered. All the while, the fraudster continues to ask for additional payments. The scammer may assert that another winner has not claimed the jackpot, and, therefore, the victim is entitled to additional payments as soon as the additional taxes and fees are paid. According to data collected by the FTC's Consumer Sentinel, there were nearly 90,000 consumer complaints regarding prizes, sweepstakes and lottery scams

in 2013.[47] Individual victim losses reported to the Hotline have ranged from a couple hundred dollars to over $500,000.

Investigators may refer victims of lottery scams to:

- The FTC;
- The Department of Homeland Security's ICE tip line. ICE investigates cross-border crimes and leads the Jamaican Operations Linked to Telemarketing (JOLT) task force, a multi-agency, international task force established with the goal of eradicating lottery scams;[48]
- The U.S. Postal Inspection Service, which investigates fraudulent use of the nation's mail system and has a history of actively pursuing lottery scammers;[49] and
- The AARP Fraud Fighter Call Center, which is staffed with caseworkers who are well-versed in speaking with victims and their families who are dealing with the effects of lottery scams;[50]

a. Jamaican Lottery Scams

A sophisticated and common variation of the lottery scam is known as the Jamaican lottery scam. In 2012, it was estimated that scammers in Jamaica placed 30,000 calls daily to older Americans in an effort to swindle them out of their life savings.[51] Frequently, the phone numbers displayed on Caller ID will begin with area code 876, which is Jamaica's country code, but is also often confused with an American toll-free phone number. More sophisticated scammers, however, are able to "spoof" Caller ID so that a U.S. number appears, even if the scammer is calling from overseas.[52] These scammers are often relentless in their pursuit of money. The daughter of a victim of the Jamaican lottery scam, who testified at the Committee's March 2013 hearing on the topic, explained that her father would sometimes receive 85 to 100 calls per day.[53] At times, scammers have also been known to threaten harm to a victim or his or her family. They may use readily available technology, such as Google Earth, to view images of a victim's home and neighborhood. Using this information, they can reference the appearance of the victim's home or a nearby landmark, making the scammer's claims that he or she is nearby much more believable.

According to the FTC, in 2007, there were 1,867 complaints related to Jamaican lottery scams; by 2011, the figure had ballooned

---

[47] FTC, *Consumer Sentinel Network Data Book for January–December 2013* (Feb. 2014) (online at http://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2013/sentinel-cy2013.pdf)

[48] U.S. Department of Homeland Security's Immigration and Customs Enforcement, *U.S. and Jamaica Launch International Task Force to Combat Telemarketing Fraud* (May 27, 2009) (online at http://www.ice.gov/news/releases/0905/090527kingston.htm)

[49] *See*, *e.g.*, Department of Justice, *Jamaican DJ Arrested in Florida in Connection with North Dakota Telemarketing Lottery Scam; 26 Individuals Currently Indicted* (May 27, 2014) (online at: http://www.justice.gov/usao/nd/news/2014/05-27-14-Willcocks%20Arrested.html)

[50] AARP, *AARP Fraud Fighter Call Center Dials in on Scams* (Feb. 2, 2014) (online at http://states.aarp.org/aarp-fraud-fighter-call-center-dials-in-on-scams/)

[51] Caribbean Policy Research Institute, *Background Brief: Jamaican Lottery*, p. 5 (Nov. 2012), (online at http://www.capricaribbean.org/sites/default/files/text/FINAL_Background%20Brief_Jamaican%20Lottery%20Scam_November%202012.pdf)

[52] Federal Communications Commission, *Caller ID and Spoofing* (online at http://www.fcc.gov/guides/caller-id-and-spoofing)

[53] U.S. Senate Special Committee on Aging, *876–SCAM: Jamaican Phone Fraud Targeting Seniors*, Testimony of Kim Nichols (March 13, 2013) (online at http://www.aging.senate.gov/imo/media/doc/01_Nichols_3_13_13.pdf)

to more than 30,000 complaints.[54] Experts believe that as many as 90 percent of the victims of this scam do not report their experience to authorities, often due to embarrassment and shame.[55] As a result of the underreporting of this scam, it is difficult to measure how much money has been taken from victims. According to some estimates, victims lost $300 million in 2011, up from $30 million in 2008, to Jamaican lottery scams.[56] An FTC official stated that prize and lottery scams worldwide could be bilking Americans out of as much as $1 billion a year.[57]

In the Committee's hearing to examine the Jamaican Lottery Scam, the stories of two victims of the scam were shared by their families:

- Kim Nichols told the heartbreaking story of her father, a retired commercial airline pilot who flew for 36 years after proudly serving in the U.S. Armed Forces. Over the course of approximately five months, the scammer defrauded Ms. Nichols' father out of $85,000.[58]
- After learning that her mother was sending money to fraudsters located in Jamaica in hopes of claiming a $4.2 million lottery, Sonia Ellis had to file for legal guardianship to protect her mother's remaining assets. From December 2008 to July 2012, Sonia's mother sent approximately $64,500 to scammers.[59]

A local sheriff, officials from ICE and the U.S. Postal Inspection Service, and a representative of a wire transfer service often used by victims to transmit money to scammers all shared their efforts to bring an end to the scam. The hearing also sought to press the Department of Justice (DOJ) to work toward extraditing perpetrators of the crime to the United States for trial. Chairman Nelson explained that such an action would have a chilling effect on those who now commit the crime with a sense of impunity.[60] Following the hearing, on March 15, 2013, Chairman Nelson and Ranking Member Collins wrote a letter to U.S. Attorney General Eric Holder in which they expressed their concern over the "lack of attention" being paid to the Jamaican lottery scams and urged the DOJ to work toward extraditing lottery scammers from Jamaica.[61]

---

[54] Caribbean Policy Research Institute, *Background Brief: Jamaican Lottery*, p. 5 (Nov. 2012)

[55] *Id*. at p. 5–p. 6 (Nov. 2012)

[56] David McFadden, *Jamaican Lottery Scams Spread Despite US Crackdown*, The Associated Press, (April 2012) (online at http://www.businessweek.com/ap/2012-04/D9U6Q1O00.htm)

[57] *Id*.

[58] U.S. Senate Special Committee on Aging, *876–SCAM: Jamaican Phone Fraud Targeting Seniors*, Testimony of Kim Nichols (March 13, 2013) (online at http://www.aging.senate.gov/imo/media/doc/01_Nichols_3_13_13.pdf)

[59] U.S. Senate Special Committee on Aging, *876–SCAM: Jamaican Phone Fraud Targeting Seniors*, Testimony of Sonia Ellis (March 13, 2013) (online at http://www.aging.senate.gov/download/2013/03/13/sonia-ellis-testimony-031313)

[60] Ledyard King, *U.S. Authorities Tell Nelson Indicted Jamaican Scammers will be Extradited*, Florida Today (April 25, 2013) (online at http://www.floridatoday.com/article/20130424/NEWS01/130424027/U-S-authorities-tell-Nelson-indicted-Jamaican-scammers-will-extradited)

[61] U.S. Senate Special Committee on Aging, *Lawmakers Press Justice Department to Extradite Lottery Scammers* (March 15, 2013) (online at http://www.aging.senate.gov/press-releases/lawmakers-press-justice-department-to-extradite-lottery-scammers)

Hotline Success Story: Jamaican Lottery Scam

Earlier this year, Committee staff received a call from a married couple, both seniors, who were victims of a Jamaican lottery scam. Over the previous year, they had sent more than $100,000 to Jamaican fraudsters. Recognizing the special facts in this case, in addition to providing the couple with contact information for the relevant law enforcement agencies, Committee staff also collected the detailed information retained by the victims and shared these facts directly with Federal law enforcement officials. In the past six months, nearly a dozen individuals involved in the scam have been identified, including one fraudster who makes frequent trips to the United States, likely to collect money from middlemen. Unfortunately, as is typical with this scam, it is unlikely that the victims will be able to recover any money; however, due to the laws passed in Jamaica following the Committee's hearing last year, if convicted in the Jamaican judicial system, the scammers could face jail time and fines.

According to the Jamaican government, as of February 2014, more than 100 arrests had been made under the anti-lottery scamming law, which was passed in 2013.[62] To date, no lottery scammers living in Jamaica have been extradited to the U.S. for prosecution.

The following are lottery scam victims who contacted the Hotline to report their experiences:

- William called the Hotline with concern over his father, who is continually bombarded via phone and mail by fraudsters who claim he has won $2.5 million. Since 2012, he has wired close to $200,000 to these scammers in an effort to claim his supposed winnings. Despite William's efforts to convince his father that it is all a scam, his father continues to believe he is the winner of $2.5 million. An investigator provided William with contact information for ICE, the U.S. Postal Inspection Service, and the AARP Fraud Fighter Call Center. The Committee also sent him a letter with information about the scam so that William could share something concrete with his father.
- Ethan's father, a retired attorney, fell victim to the Jamaican lottery scam. Although Ethan was granted temporary conservatorship over his father's finances, his father continues to send whatever money he can accumulate to the scammers, who call him multiple times a day from Jamaican phone numbers. According to Ethan's calculations, his father has lost over $500,000 to this scam. An investigator referred Ethan to the AARP Fraud Fighter Call Center and to the ICE tip line. Ethan was also provided the link to the Committee's hearing for more information on the Jamaican lottery scam.

---

[62] Jamaica Information Service, *More Than 100 Scammers Arrested* (Feb. 6, 2014) (online at http://jis.gov.jm/10009scammers-arrested/)

• After discovering her parents lost $180,000 to the Jamaican lottery scam, Alice had to take over her parents' finances and confiscate their phones. After sending most of the money they had saved for retirement, Alice's parents eventually sold their home to send the proceeds to the scammers. Alice's father passed away soon after finding out it was a scam, and her mother is still in denial. An investigator spoke with Alice and provided her with the contact information for the ICE tip line, the AARP Fraud Fighter Call Center and to Western Union's Fraud Hotline since a majority of the money was sent using Western Union's wire transfer service. Furthermore, the investigator spoke with a sergeant at the county police department to follow up with Alice and ensure all steps have been taken to investigate the scam.

• Elizabeth from Florida is receiving numerous calls a day from Jamaican lottery scammers. She has not fallen victim to this scam, but she is worried her neighbors have. Although she knows this is a scam and has asked the scammers to stop calling, they continue to call her daily. She has contacted her local telephone company, and they have tried to stop the phone calls; however, as soon as she blocks one phone number, the scammers begin calling from a new number. Elizabeth was provided with contact information for the ICE tip line and the FTC. She was also sent the Committee's Jamaican lottery scam letter for information on this scam to share with her neighbors.

VII. SOCIAL SECURITY FRAUD

As Social Security payments have moved from mailed checks to electronic payments via direct deposit or debit card, a new type of fraud has emerged. Fraudsters use banks and debit cards to set up accounts to which they can re-route Social Security benefits from the rightful recipients to these fraudulently created accounts. As of November 30, 2014, the SSA Office of Inspector General (SSA OIG) reported it had received more than 42,000 allegations of questionable changes to a beneficiary's account. Many seniors rely on Social Security benefits for a large percentage of their income, resulting in drastic changes in everyday life for a senior who is the victim of Social Security fraud. Almost 90 percent of people age 65 and over receive some of their family income from Social Security, and without Social Security benefits, 44.4 percent of Americans 65 and over would have incomes below the poverty line.[63] Without their monthly benefits, these seniors would be unable to purchase basic day-to-day necessities.

The SSA OIG found that fraudsters most commonly make changes to the way in which Social Security benefits are to be paid through financial institutions, often directing the benefits to prepaid debit cards. Fraudsters also go online to establish a *My Social Security* account, which is an online tool that allows Social Security recipients to access information about their benefits and change payment information. As of January 2013, SSA reported that more

[63] Center on Budget and Policy Priorities, *Social Security Keeps 22 Million Americans Out of Poverty: A State-By-State Analysis* (Oct. 2013) (online at http://www.cbpp.org/cms/?fa=view&id=4037)

than 22,000 potentially fraudulent *My Social Security* accounts had been opened.[64]

On June 19, 2013, the Committee held a hearing titled "Social Security Payments Go Paperless: Protecting Seniors from Fraud and Confusion." The hearing examined what actions have been taken by SSA and the Treasury Department to prevent Social Security benefit fraud during the transition to electronic payments.[65]

Callers reporting Social Security fraud may be handled in the following ways:

- In cases where their Social Security benefits were fraudulently misappropriated, victims who require their benefits to pay for basic necessities are directed to their local SSA office to file for what is known as a critical payment, which usually provides a beneficiary with a paper check on the spot; and
- Callers who suspect fraudulent use, waste or abuse in Social Security programs and operations are encouraged to contact the SSA OIG to file a report.

The Hotline reports of Social Security fraud include the following:

- A Florida senior named Julia discovered that her daughter had been taking her Social Security disability benefits for months, so she opened a new bank account and requested that her benefits be deposited to that account. When Julia's daughter learned that her mother had set up a separate account, she contacted SSA to again redirect the benefits back to the old account. Julia's relative contacted the Hotline in search of information about how she could stop Julia's daughter from continuing to steal her benefits. An investigator referred Julia's relative to Julia's local SSA office and advised her to request that a freeze be placed on Julia's Social Security account, which will prevent any future changes to the account information unless Julia physically visits her local SSA office. Further, she was provided with the contact information for the SSA OIG to report the fraudulent use of her Social Security benefits.
- Anna became worried that she was the victim of Social Security fraud when her monthly benefit did now show up in her bank account. Anna contacted SSA and found out that someone had changed the address and direct deposit information on her account. Anna is a senior living in Arizona who depends on her monthly Social Security benefits to pay for rent and groceries. Anna was referred by an investigator to her local SSA field office, where she could place a freeze on her account and file for a critical payment. She was also encouraged to contact the SSA OIG to report the fraudulent use of her Social Security benefits.
- After receiving a letter thanking him for opening an online account with Social Security, James, an Illinois resident, realized he was a victim of Social Security fraud. A scammer had created a *My Social Security* account in his name and then used it to request that his Social Security check be direct deposited into a bank account located in another state. Because James was proactive and

[64] U.S. Senate Special Committee on Aging, *Social Security Payments Go Paperless: Protecting Seniors from Fraud and Confusion* (June 19, 2013) (online at http://www.aging.senate.gov/imo/media/doc/05_SSA_IG_O'Carroll_6_19_13.pdf)

[65] Almost all Social Security beneficiaries have been required to receive their Social Security benefits electronically since March 1, 2013 (see explanation at http://www.ssa.gov/deposit/)

contacted the SSA immediately, the fraud was discovered and his local Social Security office was able to correct the information. James contacted the Hotline to share his experience.

VIII. TIMESHARE SCAMS

Given the significant drop in the value of numerous timeshares in recent years, many timeshare owners are desperate sell their units, especially older Americans, who may no longer be able to use a timeshare, but must continue to pay the compulsory annual maintenance fees. Scammers contact timeshare owners claiming to have found someone interested in buying the timeshare. The owner is told he must simply pay transfer fees and closing costs, which the scammer may claim will be refunded upon completion of the sale. Victims pay anywhere from a few hundred to many thousands of dollars in hopes of closing the sale. According to Lois Greisman, the Associate Director of the Division of Marketing Practices at the FTC, "there are tens of millions of dollars being bilked from people who are trying to unload their properties because they need the money." [66]

In 2013, the FTC Consumer Sentinel logged 30,094 complaints related to travel, vacations and timeshare plans.[67] In a two-year period, U.S. and Florida officials filed nearly 200 civil and criminal cases in the state of Florida.[68] One case, brought by the Southern District of Illinois U.S. Attorney's Office, involved a massive timeshare fraud that bilked more than 22,000 victims from 50 states out of over $30 million.[69] The fraud ring grew from four employees to nearly 300, with nine locations across Florida. Losses to timeshare scams reported to the Hotline have ranged from $250 to over $19,000.

Victims of a timeshare scam are typically encouraged to report the fraud to:

- The office of their state Attorney General and any relevant state consumer protection agency;
- The FTC; an
- The IC3, if the victim responded to an Internet ad for timeshare resale services.

Complaints to the Hotline include:

- Susan in Virginia reported receiving a call from an individual claiming to be from the company "Timeshares by Owner," who said he had a buyer ready to purchase her timeshare and needed a payment of $1,500 to cover closing costs. She was even placed on the phone with an individual who claimed he was the interested buyer, but, as soon as she sent a payment, the scammer stopped answering her calls. An investigator provided Susan with contact information for the FTC and the Virginia Attorney General's office.

---

[66] Herb Weisbaum, *Timeshare Resale Scams Take In Millions*, Today Money (April 2012) (online at http://www.today.com/money/timeshare-resale-scams-take-millions-667476)

[67] FTC, *Consumer Sentinel Network Data Book for January–December 2013* (Feb. 2014) (online at http://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2013/sentinel-cy2013.pdf)

[68] Susannah Nesmith, *Florida, U.S. Crack Down on Timeshare Fraud*, Bloomberg (June 2013) (online at http://www.bloomberg.com/news/2013-06-06/florida-prosecutors-say-191-timeshare-cases-filed-in-crackdown.html)

[69] Andrea Day and Valerie Patriarca, *Dream Vacation Turned Timeshare Nightmares,* CNBC (March 20, 2014) (online at http://www.cnbc.com/id/101488801)

• Marge in Florida was repeatedly victimized by scammers claiming to have buyers lined up for her timeshare. She explained to an investigator that her desperation to get rid of the timeshare led her to believe the fraudsters as they kept asking for additional payments to ensure the sale could be finalized. She eventually lost approximately $10,000, and her timeshare was never sold. Marge was advised to report this scam to her Attorney General's office, the Florida Department of Agriculture and Consumer Services and the FTC.

IX. FRAUD INVOLVING GUARDIANSHIP

The purpose of a court-appointed guardianship is to protect and exercise the legal rights of an individual who has been deemed to lack the capacity to handle his or her own affairs. A guardian can be a family member or friend, a public guardian appointed by the state, or a private guardian if the individual is able to provide compensation. State courts are responsible for overseeing guardians, and laws pertaining to guardianships may vary greatly from one state to another.[70] Individuals have contacted the Hotline to share heartbreaking stories of the abuses they have witnessed within the guardianship system, typically involving financial abuse of an elderly individual.

Individuals who have contacted the Hotline for assistance with guardianship issues are often referred to state authorities. The Department of Justice's Elder Justice Initiative is also a valuable resource, providing state-by-state information for victims of financial exploitation and their families, practitioners who serve them, and prosecutors and law enforcement agencies.[71]

Individuals who have contacted the Hotline include:

• Alexandra, a resident of Missouri, explained that her father was placed under a temporary guardianship. While under the care of the guardian, Alexandra's father's assets were squandered and necessary medical care was not provided. Alexandra has contacted law enforcement and shared the evidence she has collected of the abuse inflicted by the guardian.

• Elaine, a resident of North Carolina, said that her sister's lies led to a court-appointed guardianship for her father. Elaine claims the guardian drugged and abused her father and sold his home for $1.5 million, taking all the money for himself. While one state organization says it is investigating what happened to Elaine's father, no action has been taken by state or federal authorities.

• Jim, an attorney in Florida, contacted the Hotline because he believed the Social Security benefits of a client were being misappropriated by a representative payee,[72] the client's brother. The brother is a convicted felon but neglected to notify anyone of this fact when he sought to become his brother's representative payee. Although the beneficiary was deemed mentally impaired, a bank account was set up in such a way as to ensure that, even after the beneficiary passed away, the benefits would remain in his posses-

[70] *See* U.S. Social Security Administration, *Digest of State Guardianship Laws* (Aug. 2012) (online at https://secure.ssa.gov/poms.nsf/lnx/0200502300)

[71] U.S. Department of Justice, Elder Justice Initiative (online at http://www.justice.gov/elderjustice/)

[72] A representative payee is appointed by a Federal agency to handle the benefits of an incapacitated individual

sion instead of passing to the estate. A Committee investigator put Jim in touch with one of Chairman Nelson's caseworkers in Florida and also advised Jim to contact the SSA OIG.

X. CONCLUSION

It is clear that more needs to be done to help seniors protect themselves from scams and the financial exploitation that accompanies them. With the aging of the American population, the problems highlighted in this report will only continue to grow.[73] Information gathered through the Hotline and the resulting work of the Committee have already brought about some important successes. For example, after sustained Committee pressure, two of the three primary providers of prepaid debit reload products, Green Dot and InComm, announced their plans to distoninue the PIN method of reloading prepaid cards by the end of the first quarter of 2015, citing concerns over the extent to which scam artists were utilizing them in their fraud schemes.[74] The third provider, Blackhawk, also recently unveiled enhanced security measures that it believes will mitigate the risks posed by fraud.[75] However, as illustrated by the continued daily reports of fraud to the Hotline, much more work remains to be done. The Hotline provides a glimpse into the current state of scams against older Americans—information that the Committee hopes will not only raise awareness of the extent of this scourge, but also inform the conversation as possible solutions are considered.

[73] Allianz Life Insurance Company of North America, 2014 Safeguarding Our Seniors, *New Allianz Life Study Confirms Elder Financial Abuse Under-Reported and Misunderstood Problem Likely to Grow* (Oct. 15, 2014) (online at https://www.allianzlife.com/about/news-and-events/news-releases/Press-Release-October-15-2014)

[74] U.S. Senate Special Committee on Aging, *Private Industry's Role in Stemming the Tide of Phone Scams,* Testimony of Steven W. Streit and Skeet Rolling (Nov. 19, 2014) (online at http://www.aging.senate.gov/hearings/private-industrys-role-in-stemming-the-tide-of-phone-scams)

[75] U.S. Senate Special Committee on Aging, *Private Industry's Role in Stemming the Tide of Phone Scams,* Testimony of William Y. Tauscher (Nov. 19, 2014) (online at http://www.aging.senate.gov/imo/media/doc/Tauscher_11_19_14.pdf)

Appendix 1: Selected Resources

- Computer Scams
  - Internet Crime Complaint Center
    - http://www.ic3.gov/default.aspx
  - Federal Trade Commission
    - http://www.consumer.ftc.gov/articles/0346-tech-support-scams
    - 1-877-382-4357
    - Fraudulent emails can be forwarded to spam@uce.gov
- Grandparent Scams
  - Attorneys General by State
    - http://www.usa.gov/directory/stateconsumer/index.shtml
  - Department of Homeland Security's Immigration and Customs Enforcement tip line
    - 1-866-347-2423
  - Federal Trade Commission
    - http://www.consumer.ftc.gov/articles/0204-family-emergency-scams
    - 1-877-382-4357
- Health-Related Scams
  - Office of Inspector General of the U.S. Department of Health & Human Services
    - https://forms.oig.hhs.gov/hotlineoperations/
    - 1-800-447-8477
  - Centers for Medicare & Medicaid Services
    - http://www.cms.gov/Medicare/Medicare.html
  - Medicare Rights Center
    - http://www.medicarerights.org/
    - 1-800-333-4114
  - Attorney General by State
    - http://www.usa.gov/directory/stateconsumer/index.shtml
  - Federal Trade Commission
    - 1-877-382-4357
  - Federal Communications Commission
    - http://www.fcc.gov/
    - 1-888-225-5322
- Identity Theft
  - Local police department
  - National credit bureaus
    - 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)
  - Federal Trade Commission's Division of Privacy and Identity Protection
    - 1-877-438-4338
  - Internal Revenue Service's Identity Protection Specialized Unit
    - 1-877-777-4778
  - Social Security Administration

        - 1-800-269-0271
- Lottery Scams
    - Department of Homeland Security's Immigration and Customs Enforcement tip line
        - 1-866-347-2423
    - U.S. Postal Inspection Service
        - https://postalinspectors.uspis.gov/
        - 1-877-876-2455
    - AARP Fraud Fighter Call Center
        - 1-800-646-2283
    - Federal Trade Commission
        - http://www.consumer.ftc.gov/articles/0086-international-lottery-scams
        - 1-877-382-4357
- Social Security Fraud
    - Local Social Security office
        - https://secure.ssa.gov/ICON/main.jsp
    - Social Security Administration's Office of the Inspector General
        - http://oig.ssa.gov/report
        - 1-800-269-0271
- Timeshare Scams
    - Attorneys General by State
        - http://www.usa.gov/directory/stateconsumer/index.shtml
    - Federal Trade Commission
        - 1-877-382-4357
- Guardianship Issues
    - U.S. Department of Justice's Elder Justice Imitative
        - http://www.justice.gov/elderjustice/

○