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 3

Top 10 Most-Reported Scams 4

Origin of Fraudulent Calls 5

State Attorneys General 7

Fraud Resources 8

Top Ten Types of Scams Reported to the Fraud Hotline

- 1. Social Security Impersonation Scam 12
- 2. Robocalls and Unsolicited Phone Calls 14
- 3. Sweepstakes Scams 16
- 4. Romance Scams 18
- 5. Computer Tech Support Scams 20
- 6. Grandparent Scams 22
- 7. IRS Impersonation Scam 24
- 8. Identity Theft 26
- 9. Debt Scams 28
- 10. Elder Financial Abuse 30

Top Scams by State 32

Appendix: 2019 Complete Fraud Hotline Statistics 36

References 39

Removable Poster with Tips on Avoiding Phone Scams 41

Senate Special Committee on Aging

SUSAN M. COLLINS, Maine

TIM SCOTT, South Carolina

RICHARD BURR, North Carolina

MARTHA McSALLY, Arizona

MARCO RUBIO, Florida

JOSH HAWLEY, Missouri

MIKE BRAUN, Indiana

RICK SCOTT, Florida

ROBERT P. CASEY, JR., Pennsylvania

KIRSTEN GILLIBRAND, New York

RICHARD BLUMENTHAL, Connecticut

ELIZABETH WARREN, Massachusetts

DOUG JONES, Alabama

KYRSTEN SINEMA, Arizona

JACKY ROSEN, Nevada

Dear Friends,

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

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

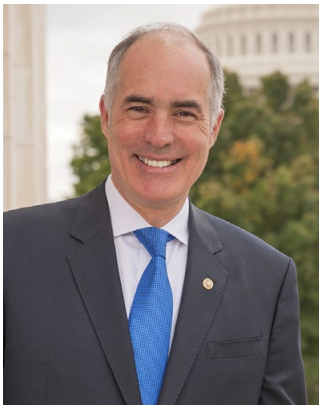
Over the past year, more than 1,300 individuals all across the country contacted the Fraud Hotline. Since the Fraud Hotline's inception in 2013, more than 9,500 individuals from all 50 states have contacted the Committee's Fraud Hotline to report a possible scam. The Committee would like to thank the many consumer advocacy organizations, community centers, and local law enforcement officials that have provided invaluable assistance by encouraging consumers to call the Fraud Hotline to document scams. We look forward to building upon our successful efforts to investigate and stop scams aimed our nation's seniors, and to ensure that federal agencies are aggressively pursuing the criminals who commit these frauds.

Sincerely,

Susan M. Collins

Susan M. Collins
Chairman

Robert P. Casey, Jr.



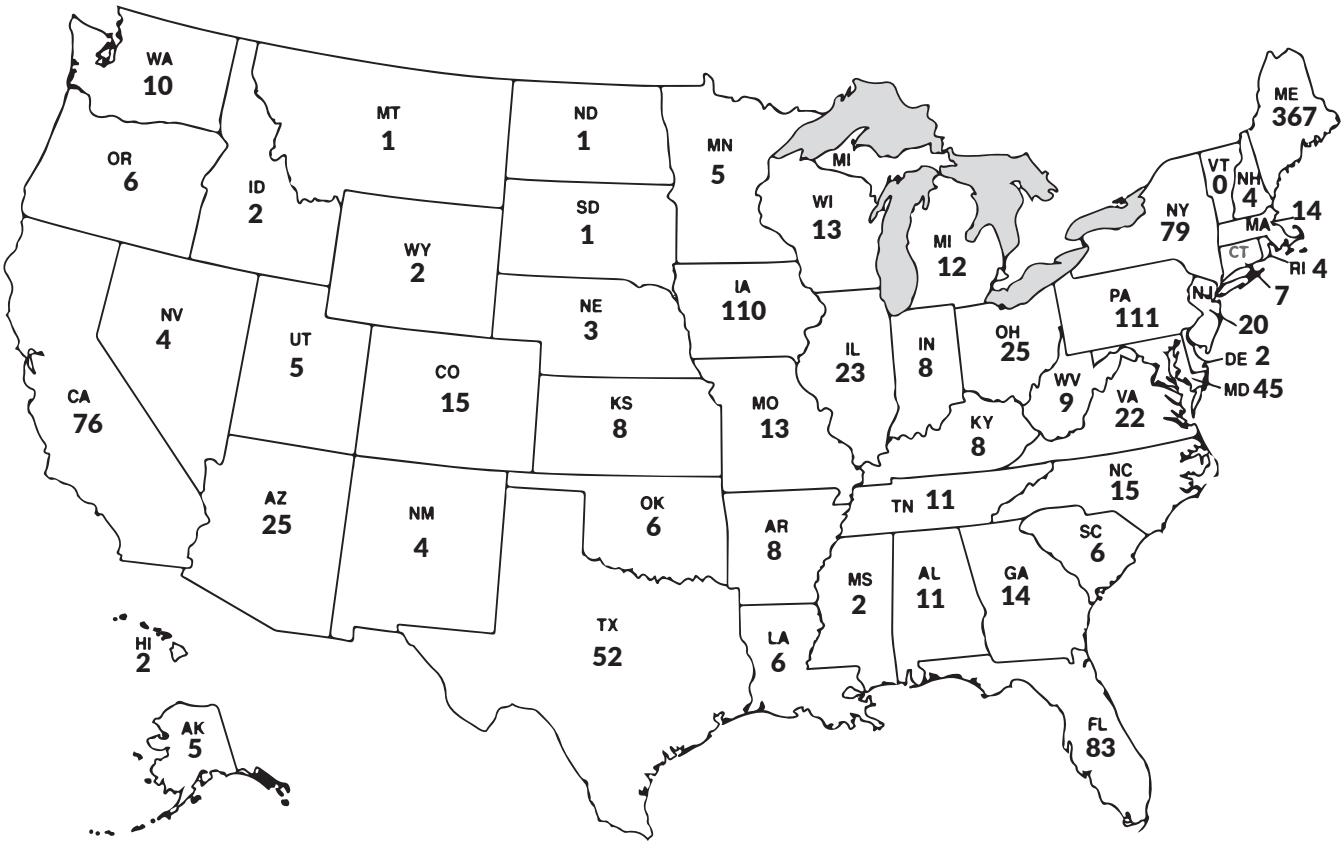
Robert P. Casey, Jr.
Ranking Member

Top 10 Most-Reported Scams

From January 1, 2019, through December 31, 2019, the Senate Aging Committee's Fraud Hotline received a total of 1,341 complaints from residents all across the country. Calls pertaining to the top 10 scams featured in this report account for more than 70 percent of the complaints.

Rank	Type of Scam	# of Complaints
1	Social Security Impersonation Scam	371
2	Robocalls / Unsolicited Phone Calls	123
3	Sweepstakes Scam / Jamaican Lottery Scam	107
4	Romance Scams	99
5	Computer Tech Support Scams	93
6	Grandparent Scams	51
7	IRS Impersonation Scam	34
8	Identity Theft	27
9	Debt Scams	21
10	Elder Financial Abuse	18

Origin of Calls Received by the Aging Committee Fraud Hotline



Abbreviations

Adult Protective Services	**APS**
Better Business Bureau	**BBB**
Department of Homeland Security	**DHS**
Department of Justice	**DOJ**
Federal Bureau of Investigation (FBI)	**FBI**
Federal Communications Commission	**FCC**
Federal Trade Commission	**FTC**
Government Accountability Office	**GAO**
Health Insurance Claim Number	**HICN**
Internal Revenue Service	**IRS**
Internet Crime Complaint Center	**IC3**
Legal Services for the Elderly	**LSE**
Personally Identifiable Information	**PII**
Social Security Administration	**SSA**
Social Security Number	**SSN**
Treasury Inspector General for Tax Administration	**TIGTA**
Voice over Internet Protocol	**VoIP**

State Attorneys General

If you think you have been defrauded by a business or had assets stolen by someone you trusted, call your state, district, or territory Attorney General's office.

Alabama
(334) 242-7300

Alaska
(907) 269-5100

Arizona
(602) 542-5025

Arkansas
(800) 482-8982

California
(916) 445-9555

Colorado
(720) 508-6022

Connecticut
(860) 808-5400

Delaware
(302) 577-8600

District of Columbia
(202) 442-9828

Florida
(850) 414-3300

Georgia
(404) 656-3300

Hawaii
(808) 586-1500

Idaho
(208) 334-2400

Illinois
(312) 814-3000

Indiana
(317) 232-6330

Iowa
(515) 281-5044

Kansas
(785) 296-3751

Kentucky
(502) 696-5300

Louisiana
(225) 326-6465

Maine
(207) 626-8800

Maryland
(410) 576-6300

Massachusetts
(617) 727-2200

Michigan
(517) 335-7622

Minnesota
(651) 296-3353

Mississippi
(601) 359-3680

Missouri
(573) 751-3321

Montana
(406) 444-2026

Nebraska
(402) 471-2682

Nevada
(702) 486-3132

New Hampshire
(603) 271-3658

New Jersey
(609) 292-8740

New Mexico
(505) 490-4060

New York
(518) 776-2000

North Carolina
(919) 716-6400

North Dakota
(701) 328-2210

Ohio
(614) 466-4986

Oklahoma
(405) 521-3921

Oregon
(503) 378-4400

Pennsylvania
(717) 787-3391

Rhode Island
(401) 274-4400

South Carolina
(803) 734-3970

South Dakota
(605) 773-3215

Tennessee
(615) 741-3491

Texas
(512) 463-2100

Utah
(800) 244-4636

Vermont
(802) 828-3173

Virginia
(804) 786-2071

Washington
(360) 753-6200

West Virginia
(304) 558-2021

Wisconsin
(608) 266-1221

Wyoming
(307) 777-7841

Puerto Rico
(787) 721-2900

US Virgin Islands
(340) 774-5666

Fraud Resources

Identity Theft

If you or someone you know have been the victim of 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)

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
USA.gov for Seniors	http://www.usa.gov/Topics/Seniors.shtml 1-800-333-4636
AARP Fraud Watch Network	www.aarp.org/fraudwatchnetwork 1-800-646-2283
FTC Sentinel Network	http://www.ftc.gov/enforcement/consumer-sentinel-network 1-877-701-9595
FTC Consumer Response Center	http://www.consumer.ftc.gov/ 1-877-382-4357
DOJ Elder Justice Initiative	www.justice.gov/elderjustice/ 1-202-514-2000 (DOJ Main Switchboard)
Area Agency on Aging	http://www.n4a.org/
IRS Scam Reporting Hotline	https://www.treasury.gov/tigta/contact_report_scam.shtml 1-800-366-4484
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

Executive Summary

U.S. Senators Susan Collins (R-ME) and Bob Casey (D-PA), Chairman and Ranking Member of the Senate Special Committee on Aging, are leading efforts to fight fraud targeting older Americans. This fraud book reports annually on the top frauds affecting seniors, and provides tips for older Americans, families, and communities to stay safe. In addition to this ongoing work, the Committee has held 24 hearings over the past seven years focused on financial fraud and scams, examining many of the frauds featured in this book. Senators Collins and Casey have also championed bills to protect seniors from scams and exploitation. The *Senior$afe Act*, a 2018 law championed by Senators Collins and Casey, helps protect older adults from financial exploitation. Also, in February 2019, the Chairman and Ranking Member reintroduced the *Guardianship Accountability Act*, which would promote guardianship oversight, while also encouraging information sharing among state and federal government entities and other relevant organizations. Further, at the urging of the Committee, the Federal Communications Commission finalized new rules between 2015 and 2019 to help put an end to illegal robocalls.

The Senate Special Committee on Aging's Fraud Hotline is a hallmark resource that is available to seniors across the country to fight fraud. The Hotline provides free support to help older adults and their families prevent frauds and scams, or report them, and work towards justice in cases when they do occur. From January 1, 2019, through December 31, 2019, the Senate Special Committee on Aging's Fraud Hotline received a total of 1,341 reports from callers throughout the United States. Calls pertaining to the top 10 scams featured in this Fraud Book accounted for 70 percent of complaints.

The Scams

1. This year, a significant change occurred in the most common phone scam plaguing seniors. Since the Committee set up the Fraud Hotline in 2013, the IRS Impersonation Scam has been the most frequent complaint. However, in 2019, the Hotline saw a marked decline in reports of the IRS scam and a large increase in reports of the **Social Security Impersonation Scam**. This scam, which was the top complaint and the focus of more than twice as many calls as any other scam, involves scammers posing as employees of the Social Security Administration in order to fraudulently take money or obtain personally identifiable information (PII) from victims. In one common version of this scam, victims are told that their Social Security number has been linked to a crime and the situation can only be resolved by sending payment or PII.

2. As in 2018, the second most common scam reported to the Fraud Hotline this year involved **robocalls or unsolicited telephone calls**. Illegal robocalls, which often originate overseas, have become an increasing nuisance to consumers due to advances in technology. Additionally, con artists often "spoof" their number to make it appear that they are calling from a government agency or legitimate business.

3. **Sweepstakes Scams**, such as the Publishers Clearing House Scam, remain a problem for seniors, placing third on the list again this year. Perpetrators of this scam aim to convince victims that they have won a large sum of money through the lottery, but must make up front payments for taxes and fees before collecting their prize. The con artists often collect large sums of money, sometimes tens or hundreds of thousands of dollars, over an extended period of time while the "winnings" never come.

4. **Romance Scams** also saw a significant increase in complaints from previous years and was the fourth most-reported complaint. Americans are often turning to online dating to find love, and scammers have taken advantage of this opportunity by creating fake online profiles to attract victims. Once a scammer has gained a victim's trust over weeks, months, or even years, the scammer requests money to pay for an unexpected bill, an emergency, or another alleged expense.

5. The fifth most-reported scam was **Computer Scams**. Although there are many variations of computer scams, fraudsters typically claim to represent a well-known technology company in an attempt to convince victims to provide them with access to their computers. Scammers often demand that victims pay for bogus technical support services through a wire transfer or obtain victims' passwords and gain access to financial accounts.

6. **Grandparent Scams** placed sixth 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. Scammers increasingly work in pairs with one briefly imitating the grandchild before quickly handing the phone off to another scammer that impersonates an authority figure, such as a police officer pretending to confirm the story or defense attorney to make the request for money.

7. Falling from number one for the first time since the Fraud Hotline was established, the **IRS Impersonation Scam** ranked seventh on the list. In this scam, IRS impersonators often accuse victims of owing back taxes that must be paid immediately. After an initial "payment" is made, con artists often convince victims to make additional payments to prevent arrest or other adverse actions.

8. **Identity Theft** was the eighth most reported consumer complaint to the Fraud Hotline in 2019. 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. Perpetrators of identity theft can disrupt a senior's life by draining their bank accounts, making unauthorized credit card charges, or stealing government benefits, such as Medicare or Medicaid services.

9. **Debt Scams** made the top 10 for the first time in 2019. While there are multiple variations on this theme, reports to the Fraud Hotline generally took one of two approaches. In the first approach, the scammer would claim that the victim owed money on their credit card and should make a payment immediately. In the second, the scammer offered to help with debt consolidation and requested the victim's personal information, which was likely used to steal the victim's identity or take money directly from their bank account.

10. **Elder Financial Abuse** placed tenth on the list this year. Reports to the Fraud Hotline focused on the illegal or improper use of an older adult's funds, property, or assets. Perpetrators can include those with close contact with the victim, such as family or paid homecare workers, or strangers.

In addition to these ten most-common scams, the Fraud Hotline also received many reports of deceptive and underhanded business practices. These consumer complaints took different forms and involved businesses in a variety of industries. Consumers should be wary of any offer that sounds too good to be true and carefully read any contract, or consult with others, before agreeing to sign. Questionable practices can be reported to state attorneys general, consumer protection agencies, and the Better Business Bureau.

How to Protect Yourself

There are several steps every senior can take to help avoid falling victim to a scam, which are outlined in this book. In summary, it is imperative that seniors stay vigilant and watch out for any efforts to steal their money. Since most scams originate with a phone call, it is important to remain aware when taking phone calls and hang up immediately if the caller sounds suspicious, makes threats, or makes an offer that sounds too good to be true but requires something from you. Additionally, it is necessary to keep personally identifiable information (PII), such as a Social Security number or bank account number, private and secure. If ever you are in doubt about an offer, call, or transaction, call the Fraud Hotline at (855) 303-9470.

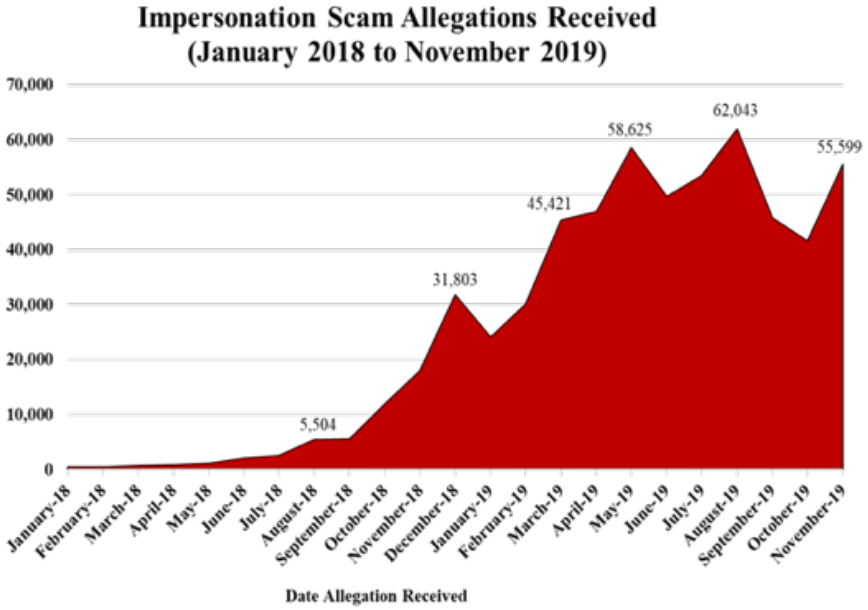
Top Ten Types of Scams

Reported to the Fraud Hotline

1 Social Security Impersonation Scam

In 2019, for the first time since the inception of the Fraud Hotline in 2013, the most-reported scam was the Social Security Impersonation Scam. While the Fraud Hotline has received reports of this con for several years, it jumped from the seventh most-reported scam of 2018 to the most-reported of 2019. In the first half of 2019, the FTC received almost double the number of Social Security Scam complaints than it received in all of 2018, with total reported losses of just under $17 million.[1]

The Social Security Impersonation Scam involves consumers receiving calls from individuals claiming to represent the Social Security Administration (SSA). The scammers often "spoof" the SSA's public numbers to make it appear as if the fraudulent call is actually coming from the SSA. While there are several variations to this scam, the general theme involves the scammers calling victims to fraudulently take money from them or obtain their personally identifiable information. In one



Source: Social Security Administration Office of the Inspector General

common iteration of the scam, the fraudsters will attempt to scare consumers by claiming that their Social Security number has been suspended due to suspicious activity or has been used in a crime. The scammers will say the situation can only be resolved by providing sensitive personal information over the phone or by paying a sum of money using a particular means of payment, such as gift cards. These tactics aim to panic the consumer by creating a false sense of urgency, and many individuals do indeed panic and give away their information and hard-earned money.

It is important to note that SSA employees occasionally reach out by telephone for customer-service purposes.[2] In only a few special situations, usually already known to the individual by previous direct contact with the agency, an SSA employee may request the confirmation of personal information over the phone. SSA warns that legitimate SSA callers will provide a telephone number and extension.[3] If you are ever confused or unsure whether you are speaking with a real SSA employee, you may request that they call you back later, after you have verified that they are legitimate by calling the SSA Inspector General's toll-free number (1-800-772-1213).

In addition to phone calls, some people have reported getting emails claiming to be from SSA. According to SSA's website, "Social Security will **not** send you an email asking you to give us your personal information, such as your Social Security number, date of birth, or other private information. If someone saying they are from Social Security does email you requesting information, don't respond to the message."[4]

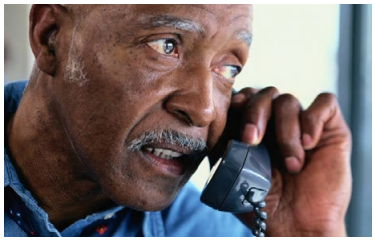
Fraud Case #1:

"Laura" from Texas called the Fraud Hotline to report receiving two calls from two scammers, one posing as her county sheriff and the other as a local police officer. They told her the same story: that there was evidence her Social Security number had been used in a complicated criminal conspiracy, and that the only way to clear her name would be to pay a fee of $20,000. The scammers instructed her to buy gift cards from Target and Macy's and read the gift card numbers over the phone. Laura complied, buying the cards and reading the numbers to the scammers. A fraud hotline investigator reported the call to the FTC for further action.

Tips to Help Avoid the Social Security Impersonation Scam:

- Never give out personal information over the phone to someone you do not know.
- SSA will never tell you that your Social Security number has been suspended.
- SSA will not call demanding an immediate payment or ask for your credit or debit card number over the phone.
- SSA will not require a specific means of payment, such as a prepaid debit card, retail gift card, or cash.
- Don't be afraid to call SSA's Inspector General at their toll free number (1-800-772-1213) to verify the caller/request.
- If you believe you have been a victim of this scam, you can report it to the SSA's Office of Inspector General online at https://secure.ssa.gov/ipff/home or on the phone 1-800-269-0271. You can also call the Aging Committee's Fraud Hotline at 1-855-303-9470

Sources: https://www.ssa.gov/news/press/releases/2019/#11-2019-2; https://oig.ssa.gov/newsroom/scam-awareness



2 Robocalls and Unsolicited Phone Calls

In 2003, Congress passed legislation creating the national Do-Not-Call registry with the goal of stopping telemarketers from interrupting Americans at all hours of the day with unwanted calls.[5] Unfortunately, 16 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. The Federal Communications Commission (FCC) highlights private analyses which estimate that there were nearly 4 billion robocalls made every month to U.S. consumers in 2018.[6] Illegal robocalls are not just annoying; scammers use them to find potential victims.

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

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 overseas. Con artists usually spoof the number from which they are calling to either mask their true identity or to take on a new one. As described in the chapter on Social Security Impersonation Scams, fraudsters spoof their numbers to make victims believe they are calling from the government or another legitimate entity. In addition, scammers are increasingly spoofing numbers to appear as if they are calling from the victims' home states or local area codes. Some spoofing technology even makes it appear as though the call is coming from the victim's own phone number.

Fraud Case #2:

"Bill" from Maine called the Fraud Hotline to report receiving a large number of unsolicited, spoofed robocalls. Bill explained how the callers claimed to be reaching out about an expired warranty on his truck and wanted his credit card information to renew the warranty. A Fraud Hotline investigator advised Bill to list his number on the national Do-Not-Call registry, and to contact his local telephone company and inquire about call-blocking features.

Robocalls have become an increasing nuisance to consumers. Phone calls used to be routed through equipment that was costly, and calling from international locations used to be difficult and expensive. Today, phone calls can be digitized and routed from anywhere in the world at virtually no cost. This is done using Voice over Internet Protocol (VoIP) technology, which sends voice communications over the Internet. Robocalling allows scammers to place thousands of calls a day at very little cost. Behind these calls are organized and sophisticated criminal enterprises, overseeing boiler room operations abroad, often in Jamaica and, increasingly, in India.[7]

To report a suspicious call, please call **1-855-303-9470**

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

Many companies also offer third-party spoofing and robodialing services. Third-party spoofing companies provide an easy-to-use computer interface or cell phone application that allows calls to be spoofed at a negligible cost.

Experts have made it clear that it is possible to fight technology with technology. To this end, the FCC partnered with industry to accelerate the development and adoption of new tools to combat robocalls. At Senators Collins and Casey's urging, the FCC also issued rules allowing phone companies to take more aggressive actions to block unwanted robocalls before they reach consumers.[8] For example, these rules allow telecommunications providers to block numbers that are not valid or that are valid but are not currently in use. Providers may also automatically block robocalls that appear to be illegal before they reach consumers, and they may offer consumers the option to block all calls from numbers not included on a pre-specified list.[9]

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.

To take these efforts a step further, in December 2019, Congress passed and the President signed into law the *Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act*. This law contains a number of provisions aimed at stemming the tide of illegal robocalls, including a provision that requires phone companies to implement technologies that verify caller-ID information in order to help consumers identify legitimate calls.

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

- Never give out – or confirm – personal information such as account numbers, Social Security numbers, mothers' maiden names, passwords or other identifying information in response to unexpected calls or if you are at all suspicious.
- If you get an inquiry from someone who says they represent a government agency, hang up and call the phone number on the government agency's website, or in the phone book, to verify the authenticity of the request.
- Use caution if you are being pressured to quickly divulge information – this is a sure sign of a scam.
- Never send money using a reloadable card or gift card.

Source: https://www.fcc.gov/fcc-alerts-consumers-about-spoofing-1-888-call-fcc-phone-number

3 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. In this scam, fraudsters generally contact victims by phone or through the mail to tell them that they have won or have been entered to win a prize. Scammers then require the victims to pay a fee to either collect their supposed winnings or improve their odds of winning the prize.[10] According to the Federal Trade Commission (FTC), the prevalence of sweepstakes scams increased by 35 percent between 2013 and 2018.[11,12] One example of such a scheme was reported in Pennsylvania by the *Lebanon Daily News,* which told of an 82-year-old man who lost $30,000 after paying "taxes" on $10.5 million in Publishers Clearing House "winnings."[13]

Sweepstakes scams start with a simple phone call, sometimes from a number beginning with "876," an area code from Jamaica. At first glance, this country code looks similar to a call coming from a toll-free American number. As with other types of scams, these scammers use "lead lists" to identify potential victims.

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

Scammers tell victims that they have won the lottery or a brand new car, and that in order for their winnings to be delivered they must first wire a few hundred dollars to cover processing fees and taxes. The criminals will often instruct their victims not to share the good news with anyone so that it will be a "surprise" when their families find out. Scammers tell victims to send money in a variety of ways, including gift cards, electronic wire transfers, money orders, and even cold hard cash.

The con artists adopt a variety of identities to keep the money coming in ever-increasing amounts and convince the victim that their winnings will

Fraud Case #3:

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

come soon if they continue to send money. Some scammers spend hours on the phone to develop a relationship with the victims and convince the victims that they care deeply for them. Victims who resist their entreaties begin receiving calls from scammers posing as American government officials, including local law enforcement, the Federal Bureau of Investigation, the Social Security Administration, and the Department of Homeland Security, asking for personal data and bank account numbers so they can "solve" the crime.

In this scam, no winnings are ever delivered, and the "winners" get nothing but more scam calls, which some victims have reported to be up to 100 calls per day, from scammers demanding additional money.

Since the Committee began investigating this issue, the Jamaican government passed new laws enabling extradition of the criminals to the United States for trial, leading to the extradition of one scammer for prosecution in the United States.[14] Several convictions have been obtained in connection with this scam.[15]

Fraud Case #4:

In July 2019, Angela Stancik, from Texas, testified at an Aging Committee hearing on phone scams. Angela explained how her grandmother, Marjorie, committed suicide after losing her life savings in a sweepstakes scam. Marjorie was promised a large cash prize by scammers operating in Costa Rica if she would pay a series of taxes and fees on her winnings. Unbeknownst to her family, Marjorie gradually gave away all of her retirement savings and took out a reverse mortgage on her home. Angela realized that her grandmother was being scammed during their last phone conversation, in which Marjorie asked Angela for $6,000 to pay the "last" fee. When Angela refused to send the money until she had looked into the "sweepstakes," Marjorie called her son (Angela's father) and secured the money from him instead. Less than one week later, Marjorie died with $69 in her bank account. The Department of Justice and Postal Inspection Service successfully traced the scam ring to their call center in Costa Rica and their headquarters in Jamaica. The scammers responsible were extradited to the U.S., tried, and sentenced to Federal Prison.

4 Romance Scams

As Americans often turn to online dating to find love, con artists are following suit, not for love but for money. Typically, scammers contact victims online either through a chatroom, dating site, social media site, or email. Con artists have been known to create elaborate profile pages, giving their fabricated story more credibility. Con artists often call 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.

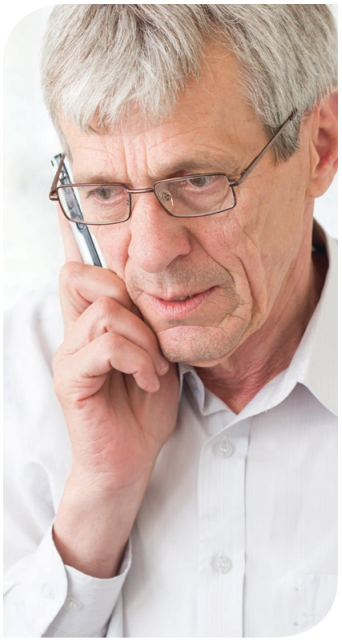
Inevitably, con artists in these scams will ask their victims for money for things such as travel expenses, surgery or medical expenses, or gambling debts.[16] Despite initially telling their victims they will never ask for any more money, romance scammers typically continue to request additional funds.

Con artists may send checks for victims to cash under the pretense that they are outside the country and cannot cash the checks themselves, or they may ask victims to forward them 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.[17]

In 2019, Federal Trade Commission's Consumer Sentinel had more than 25,000 reports about romance scams.[18]

Fraud Case #5:

"Gail" from Tennessee called the Fraud Hotline to report that she was the victim of a romance scam. A man contacted her via the online game, "Words with Friends," and they developed a romantic relationship. The man told her that he had $12 million in gold and worked on an oil rig in Nigeria, but needed her help to access it. Gail had sent the man $500,000 and depleted her retirement account before she realized that this was a scam. A Fraud Hotline investigator filed a report with the FTC and the Internet Crime Complaint Center (IC3) on her behalf.



The FBI has recommended consumers be aware of common techniques used by romance scammers, which include:

- Claiming to be from the U.S. but currently living, working, or traveling abroad.
- Claiming the romance was "destiny" or "fate," especially in early correspondence.
- Asking for money, goods, or similar types of financial assistance, especially if you have never met in person.
- Asking for assistance with personal transactions (opening a new bank account, depositing or transferring funds, shipping merchandise, etc.).

Source: https://www.ic3.gov/media/2019/190805.aspx

5 Computer Tech Support Scams

Computer-based scams involve con artists trying to gain the victims' trust by pretending to be associated with a well-known technology company, such as Microsoft, Apple, or Dell. They falsely claim that the victims' computer has been infected with a virus. Con artists convince victims to give them remote access to their computers, personal information, or credit card and bank account numbers so that victims can be "billed" for fraudulent services to fix the virus.

In a related scam, individuals searching the internet may see a pop-up window on their computer instructing them to contact a tech-support agent. Scammers sometimes use the pop-up window to hack into victims' computers, lock them out, and force 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 also spread viruses that cause the victims' computers to display error messages that instruct them to call a number to fix the problem. Scammers generally charge victims hundreds of dollars and may install free programs or trial versions of anti-virus 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."

Fraud Case #6:

"Eileen" from Massachusetts called the Fraud Hotline to report that she had lost $400,000 over the course of two years to a tech support scam. She said her computer screen froze and displayed a message offering to fix the problem and protect her computer for $300. After paying, she was contacted and told that since she didn't use the service her $300 would be refunded, but only after she sent them $700 more because they could not send a check for less than $1,000. More requests for money followed, and she paid them all via gift card. Eileen eventually called the Fraud Hotline for advice, and an investigator reported the scammer to the FTC and the FBI's Internet Crime Complaint Center (IC3). She was also eventually able to get the malware removed by the computer retailer.

- **Victims Unknowingly Contact Scammers.** Some victims unknowingly call a fraudulent tech support number after viewing the phone number online. Victims who search for tech support online may see the number for the scammer at the top of their "sponsored results." Some key search terms include: "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.
- **Fraudulent Refund.** Scammers contact victims stating that they are owed a refund for prior services. The scammers generally convince victims to provide them with access to their computers to process an online wire transfer. Instead of refunding the money, however, the fraudsters use the victims' account information to steal their savings or commit identity theft.
- **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.

The Federal Trade Commission (FTC) and the Department of Justice (DOJ) have responded to computer-based scams through investigative and enforcement actions. For example, in March 2019, the DOJ, FTC, and several state Attorneys General announced the takedown of multiple tech support schemes that collectively defrauded tens of thousands of victims in the United States.[19]

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

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

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

6 Grandparent Scams

A common scam used to target older Americans is the "grandparent scam." In this scam, imposters either pretend to be the victim's grandchild or a law enforcement officer detaining the victim's grandchild. The fraudsters claim that 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 the concerned grandparents into wiring money to them. For example, in a January 2019 Aging Committee hearing, Erika Flavin of Pennsylvania shared the story of her parents losing over $80,000 to a scammer who convinced them that their grandson had been arrested and jailed.[20]

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. Recently, the Fraud Hotline has received reports of imposter grandchildren claiming to have broken their noses in car accidents to explain why their voices sound differently. The scammer then asks the victim to help by sending money in the fastest way possible. This typically requires the victim to go to a local retailer and send an electric wire transfer of several thousand dollars, but other methods like gift cards and cash are also used.

After payment has been made, the fraudster will likely call the victim back, claiming that there was another legal fee of which they were not initially aware. In 2018 and 2019, for example, the Fraud Hotline received multiple reports of scammers initially claiming to have been in a car accident and requesting bail, then calling back and claiming that a pregnant woman was in the other car and suffered

If you are contacted by a family member who claims to be in trouble with the law or in need of other financial assistance, call their number or check with other family members before sending money to help.

Fraud Case #7:

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

a miscarriage as a result of the accident. They then begged for thousands of dollars to retain a lawyer or pay the woman off so they could avoid going to court. The second call is typically what alerts the victims that they have been scammed.

In another version of the scam, instead of the "grandchild" making the phone call, the con artist pretends to be an arresting police officer, a lawyer, or a doctor. It is also common for the con artist impersonating the victim's grandchild 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 the victim will recognize that the voice on the phone does not belong to his or her grandchild.

The Department of Justice has prosecuted cases against grandparent scammers, including a case where six defendants were sentenced to prison terms ranging from 8 months to 33 months and ordered to pay restitution for defrauding more than 250 victims of more than $750,000.[21]

Fraud Case #8:

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

7 IRS Impersonation Scam

While there are multiple variations of the Internal Revenue Service (IRS) impersonation scams, criminals generally accuse victims of owing back taxes and penalties. They then threaten retaliation, such as home foreclosure, arrest, and deportation if immediate payment is not made by certified check, electronic wire transfer, or gift card.

Fraud Case #9:

"Ellen" from California contacted the Fraud Hotline to report that her mother in-law had been the victim of the IRS scam multiple times. Her mother believed the scammers' threats that FBI and IRS investigators would soon arrest her if she did not pay back taxes that she in fact did not owe. She wired over $100,000 dollars to overseas addresses before Ellen realized what was going on. A Fraud Hotline investigator filed a report with TIGTA and the FTC.

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

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

To address this scam, the U.S. Treasury Inspector General for Tax Administration (TIGTA) and Department of Justice (DOJ) launched a joint investigation to identify the scam's perpetrators and bring them to justice. The largest enforcement action came on October 27, 2016, when TIGTA and DOJ announced that 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.[22] Between 2012 and 2016, these scammers successfully targeted 15,000 victims and made hundreds of millions of dollars by posing as IRS agents.

Fraud Case #10:

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

In addition to pursuing the scam's perpetrators, TIGTA has partnered with industry to disrupt scam attempts. Specifically, TIGTA worked with telecommunications companies to prevent scammers from spoofing the IRS' numbers and with gift card retailers to post warning signs near gift cards to alert potential scam victims of the scam before purchasing gift cards.

Although the IRS impersonation scam was the most frequent scam reported to the Committee's Fraud Hotline between 2014 and 2018, TIGTA data suggests that scammers have switched tactics and reports of this particular scam decreased significantly in 2019. For example, in September 2019, TIGTA identified a total of 11 victims, down from an average of 150 to 200 victims *per week* during the scam's peak.[23]

Fraud Case #11:

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

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

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

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

8 Identity Theft

Identity theft is a wide-ranging category that includes calls about theft of a wallet or mail, online impersonation, or other illegal efforts to obtain a person's identifiable information. Identity thieves not only disrupt the lives of individuals by draining bank accounts, making unauthorized credit card charges, and damaging credit reports, but 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.

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 or email address and correctly guessing their password. This is often referred to as an "account takeover." Whether the thief uses this method to access an existing account or uses stolen personal information to create a new account, the end result is often the same: early in the tax filing season, the thief files a false tax return using a victim's identity and directs the refund to his own mailing address or bank account. The victim only discovers this theft when they file their own return and the IRS refuses to accept it because a refund has already

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

What to Do *Right Away:*

1. **Call the companies** where you know the fraud occurred.
2. **Place a fraud alert** with a credit reporting agency and get your credit report from one of the three national credit bureaus.
3. **Report identity theft** to the Federal Trade Commission.
4. **File a report** with your local police department.

What to Do *Next:*

1. **Close new accounts** opened in your name.
2. **Remove bogus charges** from your accounts.
3. **Correct** your credit report.
4. **Consider** adding an extended fraud freeze.

Source: https://www.identitytheft.gov

Fraud Case #12:

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

Fraud Case #13:

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

been issued. In November 2015, the IRS reversed a long-standing policy and now provides victims with copies of the fake return upon written request.[24] The documents provide victims with details to help them discover how much of their personal information was stolen.

Medical identity theft occurs when someone steals personal information – an individual's name, SSN, or health insurance claim number (HICN) – to obtain medical care, buy prescription drugs, or submit fake billings to Medicare. Medical identity theft can disrupt lives, damage credit ratings, and waste taxpayer dollars. For example, in June of 2019, the Fraud Hotline received reports of scam artists attending public events in Maine and offering seniors free cheek swabs for genetic testing. The scammers claimed these tests were covered by Medicare and collected Medicare and SSNs from their customers but in fact, Medicare did not cover these tests. While the Centers for Medicare & Medicaid Services were able to prevent the federal government from being defrauded by false claims from the scammers in this case, the victims' personally identifiable information ended up in the hands of criminals that may attempt to impersonate them.

The 2017 Equifax data breach may have exposed private information belonging to more than 145 million people – nearly half the U.S. population.[25] Scammers have capitalized on the breach through robocalls claiming to be calling from Equifax to verify account information.[26] The scammers try to trick victims into sharing personally identifiable information, such as their SSNs.

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.

9 Debt Scams

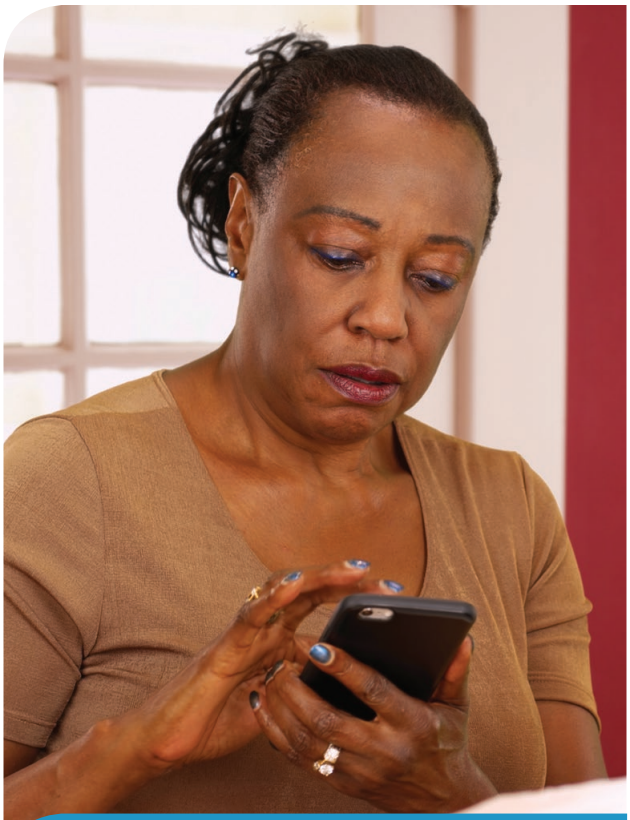
Debt collection and credit card scams ranked in the Top 10 for the first time in 2019. These scams are a growing problem for consumers, including seniors. While there are multiple variations on this theme, reports to the Fraud Hotline generally took one of two approaches: claiming potential victims owe a credit card payment or offering to help with debt consolidation.

Late Credit Card Payments

In the first approach, seniors reported scammers accusing them of owing payments on their credit cards. They then threatened retaliation (such as cancellation of the credit card, damage to the victim's credit score, or arrest) if immediate payment was not made by certified check, electronic wire transfer, or gift card. Once victims made an initial payment, they were told that further review of their credit records had identified another discrepancy and that they must pay more money or else face arrest or other adverse action. Scammers often hooked victims through this process multiple times.

Debt Consolidation Offers

In the second approach, consumers reported that scammers offered to help them consolidate their debt and asked for personal information (such as the victim's Social Security number, credit card number, or bank information). This information was likely used to steal the victim's identity or steal directly from their bank account. In some cases, scammers claimed that they provided financial advice and the victim owed them a fee to justify charging the victim's credit card or taking money from the victim's account.



Fraud Case #14:

"Amy" from Maryland called the Fraud Hotline to report that she received a call from a supposed financial advisor offering to consolidate her debt for a fee of $3,500. The "advisor" claimed to work for an investment coaching firm. Over the course of a long and rambling conversation, Amy revealed different segments of her credit card number. The scammer mailed her a contract, which she reviewed and decided not to sign. Despite not signing the contract, Amy found a $3,500 charge on her credit card. She realized that the caller had pieced together her credit card number from their conversation and called him back to demand a refund. They offered to pay back 35% of the "fee" if she would sign a liability waiver. A Fraud Hotline investigator filed a report with TIGTA and the FTC.

The debt scam calls, like others discussed in this book, often use a disguised, or "spoofed," caller identification (caller-ID) number to make the victim believe that the call is coming from a legitimate company. For example, in the late credit card payment iteration of this scam, scammers often spoof their number to make it appear that they are calling from a credit card company, such as Visa, Mastercard, or American Express. Scammers have also used this technique to make it appear as though they are calling from a local law enforcement agency. When the unsuspecting victims see the "Visa," "Mastercard," or the name of the local police department appear on their caller-IDs, they are often willing to follow the supposed debt collector's instructions to resolve the alleged credit issue.

A Few Simple Steps to Stay Safe Financially:

- Never share your credit card or bank account information over the phone, especially if you did not initiate the call.
- You may request a free credit report each year. It is recommended that you do so.
- Protect personal data. Shred unneeded bank statements, canceled checks, and credit card applications.
- If traveling, request a vacation hold on your mail or ask a trusted neighbor to pick it up.

Source: U.S. Postal Inspection Service

10 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 the Government Accountability Office (GAO), seniors lose an estimated $2.9 billion annually due to financial exploitation, although these numbers are likely too low as the crime is substantially underreported.

The Fraud Hotline documents complaints of elder abuse and refers calls to the local Adult Protective Services (APS) agencies for further action. APS employees receive reports of alleged abuse, investigate these allegations, determine whether the alleged abuse can be substantiated, or arrange for services to ensure victims' well-being.[27] APS can also refer cases to law enforcement agencies or district attorneys for criminal investigation and prosecution.[28]

Older Americans are particularly vulnerable to financial exploitation because financial decision-making ability can decrease with age. Most victims are between the ages of 80 and 89, live alone, and require support with daily activities.[29] Perpetrators may include family members, paid homecare workers, those with fiduciary responsibilities (such as financial advisors or legal guardians), or strangers who defraud older adults through mail, telephone, or Internet scams.[30]

Victims whose assets were taken by family members typically do not want their relatives to be criminally prosecuted, leaving civil actions as the only mechanism to recover stolen assets.[31] Money that is stolen is rarely recovered, which can undermine victims' ability to support or care for themselves.

The Aging Committee has brought to light many schemes that have defrauded seniors out of their hard-earned 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 advisor.

Fraud Case #15:

"Emily" from Texas called the Fraud Hotline to report that her parents had been exploited by her nephew. Her nephew feigned affection for her parents, who were living with dementia, and convinced them to allow him access to their property and credit cards over the course of more than a year. Emily's nephew proceeded to quickly drain their life savings by opening credit cards and maxing them out, as well as by selling their properties and belongings. Emily's nephew then agreed to incrementally pay back what he had spent, but he tricked her parents and recorded them agreeing over the phone that he did not need to pay them back. A Fraud Hotline investigator advised Emily about legal action and other local resources to help with restitution.

Other Activity to Watch Out For

In addition to these ten most-common scams, the Fraud Hotline also received reports of deceptive business practices. These consumer complaints took various forms and involved businesses in several different industries.

Timeshare Resale Schemes

The most common consumer complaint involved companies selling timeshares, or vacation properties, to seniors. Fraud Hotline investigators received reports of timeshare companies holding "information sessions" at retirement communities and senior centers. Salespeople would aggressively pressure seniors to sign contracts locking them into timeshare agreements, telling them the agreements would be easy to exit if the consumer was not satisfied. In some cases, seniors were harassed as they attempted to leave the session and pressured to sign on their way out. Those who did sign the contracts soon discovered that the properties were not as advertised and were difficult to resell or even sell back to the company if they no longer wanted the property or could no longer afford to make payments.

Charging a Fee for Free Services

Another variation on these complaints involved individuals pretending to provide a service or offering to help with accessing benefits for a fee. The Fraud Hotline received reports of salespeople going door-to-door in retirement communities and offering to help seniors apply for Medicare or other federal programs. The salespeople would offer to "help complete and submit" the application for them in exchange for a fee. After collecting the fee, however, these con artists would mail a blank application to the senior with the address to submit it to the appropriate agency, essentially charging a fee for printing and mailing a document available to seniors at no cost.

Sometimes these financial services or advice schemes are targeted particularly at Veterans. For example, some may try to convince older Veterans to restructure their assets to an annuity, trust, or other financial product in order to qualify for a home-based services benefit through the U.S. Department of Veterans Affairs, known as "Aid and Attendance." Restructuring assets in this way may cause the Veteran to lose access to their invested funds for a significant period of time, perhaps beyond the life of the Veteran. It is also possible that the Veteran will not even qualify for the benefit after all.

Consumers should be wary of any offer that sounds too good to be true and carefully read any contract before agreeing to sign. When in doubt, check with a family member or friend before accepting the offer or signing the contract. If a federal agency is involved, consumers can call the agency at their public phone number and check to see if a service is legitimate. Questionable practices can be reported to state attorneys general, consumer protection agencies, and the Better Business Bureau. Contact information for each State's Attorney General can be found on Page 7 of this book.

Tips from the Federal Trade Commission to Help Avoid Timeshare Resale Schemes:

- **Check out the reseller.** Contact the State Attorney General and local consumer protection agencies in the state where the reseller is located to see if there are any complaints on file.
- **Ask about fees.** If the fees must be paid in advance, get all refund policies in writing.
- **Get all details in writing.** The contract should include all services the reseller will perform and any associated fees. If the deal isn't what you wanted or expected, do not sign the contract.

Source: https://www.consumer.ftc.gov/blog/2018/05/timeshare-resale-scheme-preyed-older-adults

Top Scams by State

These scams are based on calls into the Aging Committee's Fraud Hotline in 2019.

Alabama
1. Social Security Impersonation Scam
2. Romance Scams
3. Computer Tech Support Scams
4. Consumer-Related
5. Government Grant Scam

Alaska
1. Social Security Impersonation Scam
2. Sweepstakes Scams

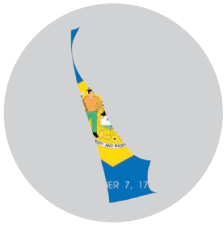
Arizona
1. Social Security Impersonation Scam
2. Computer Tech Support Scams
3. Grandparent Scam
4. Romance Scams
5. Inheritance Scams

Arkansas
1. Timeshare Scams
2. Computer Tech Support Scams
3. Sweepstakes Scams
4. Social Security Impersonation Scam
5. Unsolicited Phone Calls

California
1. Social Security Impersonation Scam
2. Romance Scams
3. Sweepstakes Scams
4. Bank Fraud
5. Identity Theft

Colorado
1. Sweepstakes Scams
2. Social Security Impersonation Scam
3. Romance Scams
4. Bank Fraud
5. Identity Theft

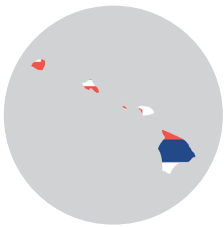
Connecticut
1. Social Security Impersonation Scam
2. Grandparent Scam
3. Robbery/Theft



Delaware
1. Payday Lending
2. Debt Collection

Florida
1. Social Security Impersonation Scam
2. Romance Scams
3. Sweepstakes Scams
4. Consumer-Related
5. Grandparent Scams

Georgia
1. Social Security Impersonation Scam
2. Romance Scams
3. Sweepstakes Scams
4. Inheritance Scams
5. Computer Tech Support Scams



Hawaii
1. Computer Tech Support Scams
2. Sweepstakes Scams

Idaho
1. Consumer-Related
2. Impending Lawsuit Scam

Illinois

1. Social Security Impersonation Scam
2. Sweepstakes Scams
3. Legal Referrals
4. Romance Scams
5. Check Scams

Maryland

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

Indiana

1. Romance Scams
2. Timeshare Scams
3. Social Security Impersonation Scam
4. Sweepstakes Scams
5. Robbery/Theft

Massachusetts

1. Unsolicited Phone Calls
2. Social Security Impersonation Scams
3. Sweepstakes Scams
4. Computer Tech Support Scams
5. Mail Fraud

Iowa

1. Social Security Impersonation Scam
2. Romance Scams
3. Grandparent Scams
4. Health-Related Scams
5. Mail Fraud

Michigan

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

Kansas

1. Social Security Impersonation Scam
2. Romance Scams
3. Grandparent Scams
4. Sweepstakes Scams
5. Check Scams

Minnesota

1. Romance Scams
2. Sweepstakes Scams
3. Computer Tech Support Scams

Kentucky

1. Social Security Impersonation Scam
2. Romance Scams
3. Inheritance Scam
4. Bank Fraud
5. Identity Theft

Mississippi

1. Utility Scam
2. Romance Scams

Louisiana

1. Sweepstakes Scams
2. Social Security Impersonation Scam
3. Inheritance Scams
4. Timeshare Scams

Missouri

1. Social Security Impersonation Scam
2. Sweepstakes Scams
3. Consumer-Related
4. Inheritance Scam
5. Durable Medical Equipment

Maine

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

Montana

1. Social Security Impersonation Scam

Top Scams by State (Cont.)

These scams are based on calls into the Aging Committee's Fraud Hotline in 2019.

Nebraska

1. Social Security Impersonation Scam
2. Sweepstakes Scams
3. Computer Tech Supports Scams

North Carolina

1. Sweepstakes Scams
2. Computer Tech Support Scams
3. Romance Scams
4. Grandparent Scams
5. Consumer-Related

Nevada

1. Romance Scams
2. Investment Fraud
3. Health-Related Scams

North Dakota

1. Sweepstakes Scams

New Hampshire

1. Unsolicited Phone Calls
2. Consumer-Related
3. Romance Scams
4. Robbery/Theft

Ohio

1. Social Security Impersonation Scam
2. Unsolicited Phone Calls
3. Sweepstakes Scams
4. Durable Medical Equipment Scam
5. Grandparent Scams

New Jersey

1. Social Security Impersonation Scam
2. Sweepstakes Scams
3. Romance Scams
4. Check Scams
5. Computer Tech Spport Scams

Oklahoma

1. Bank Fraud
2. Legal Referrals
3. Romance Scams
4. Sweepstakes Scams
5. Elder Abuse

New Mexico

1. Sweepstakes Scams
2. Debt Collection Scams
3. Timeshare Scams
4. Romance Scams

Oregon

1. Social Security Impersonation Scam
2. Identity Theft
3. Grandparent Scams
4. Elder Abuse
5. Timeshare Scams

New York

1. Social Security Impersonation Scam
2. Romance Scams
3. Sweepstakes Scam
4. Timeshare Scams
5. IRS Impersonation Scams

Pennsylvania

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

Top Scams by State (Cont.)

These scams are based on calls into the Aging Committee's Fraud Hotline in 2019.

Rhode Island

1. Inheritance Scam
2. Unsolicited Phone Calls
3. Debt Collection
4. Bank Fraud

Vermont

1. IRS Impersonation Scam

**Since the Fraud Hotline did not receive any calls from consumers in Vermont between 2018 and 2019, this list is based on call data from 2016 and 2017.*

South Carolina

1. Sweepstakes Scams
2. Social Security Impersonation Scam
3. Romance Scams
4. Computer Tech Support Scams

Virginia

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

South Dakota

1. Consumer-Related

Washington

1. Social Security Impersonation Scam
2. Grandparent Scams
3. Romance Scams
4. Consumer-Related
5. Unsolicited Phone Calls

Tennessee

1. Unsolicited Phone Calls
2. Computer Tech Support Scams
3. Sweepstakes Scams
4. Robbery/Theft
5. Impending Lawsuit Scam

West Virginia

1. Social Security Impersonation Scam
2. Romance Scams
3. Unsolicited Phone Calls
4. Sweepstakes Scams

Texas

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

Wisconsin

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

Utah

1. Social Security Impersonation Scam
2. Sweepstakes Scams
3. Identity Theft
4. Elder Abuse
5. Romance Scams

Wyoming

1. Sweepstakes Scams
2. Impending Lawsuits

Appendix: 2019 Complete Aging Fraud Hotline Statistics

Scam Type	Total
Social Security Scam	371
Unsolicited Phone Calls	123
Sweepstakes Scam	111
Romance Scam	99
Computer Scam	93
Grandparent Scam	51
Consumer related	37
IRS Scam	34
ID Theft	27
Timeshare Scam	27
Debt collection	21
Elder abuse	18
Bank fraud	18
Inheritance scam	17
Check scam	17
Health related scam	16
Mortgage Fraud	16
Impending Law Suits	15
Government Grant	12
Charity scam	11
DME Scam	11
Legal Referral	10
Robbery / theft	10
Utility scams	10
Investment fraud	7
Phishing scam	7
Home improvement scam	4
Payday lending	4
Can you hear me?	2
Long term care	2
Mail Scam	2
Grand jury impersonation	1
Western Union settlement claim	1
Miscellaneous**	32
TOTAL	**1341**

State	Total
Alabama	11
Alaska	5
Arizona	25
Arkansas	8
California	76
Colorado	15
Connecticut	7
Delaware	2
Florida	83
Georgia	14
Hawaii	2
Idaho	2
Illinois	23
Indiana	8
Iowa	110
Kansas	8
Kentucky	8
Louisiana	6
Maine	367
Maryland	45
Massachusetts	14
Michigan	12
Minnesota	5
Mississippi	2
Missouri	13

State	Total
Montana	1
Nebraska	3
Nevada	4
New Hampshire	4
New Jersey	20
New Mexico	4
New York	79
North Carolina	15
North Dakota	1
Ohio	25
Oklahoma	6
Oregon	6
Pennsylvania	111
Rhode Island	4
South Carolina	6
South Dakota	1
Tennessee	11
Texas	52
Utah	5
Virginia	22
Washington	10
West Virginia	9
Wisconsin	13
Wyoming	2
Unknown	56

Appendix: Cut out Scam Prevention Tip Cards

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

Tips from the United States Senate Special Committee on Aging for
Avoiding Scams

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

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

Tips from the United States Senate Special Committee on Aging for
Avoiding Scams

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

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


UNITED STATES
SENATE


UNITED STATES
SENATE

References

1 Hayashi, Yuka, "Social Security Adds to Capital One Hack Concern," *Wall Street Journal*, July 31, 2019 (accessed December 4, 2019) at https://www.wsj.com/articles/social-security-scams-add-to-capital-one-hack-concern-11564582509

2 Social Security Administration, "Social Security Administration and its Inspector General Announce New Online Reporting Form for Imposter Scam Calls," press release, November 19, 2019 (accessed December 4, 2019) at https://www.ssa.gov/news/press/releases/2019/#11-2019-2

3 Is that Phone Call From Us? (2017, October 30). Retrieved January 8, 2020, from https://blog.ssa.gov/is-that-phone-call-from-us/

4 Social Security Administration, "Information About Scams," *SocialSecurity.gov*, accessed December 4, 2019, at https://www.ssa.gov/phila/scams.htm

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

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

7 Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations briefing to Aging Committee Staff (2020, January 21).

8 Federal Communications Commission, "FCC Affirms Robocall Blocking By Default To Help Protect Consumers," June 6, 2019 (accessed October 30, 2019), https://docs.fcc.gov/public/attachments/DOC-357852A1.pdf.

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

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

11 Federal Trade Commission; "Consumer Sentinel Network Data Book for January-December 2015," February 2016 (accessed November 20, 2019), p. 83, at https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2015/160229csn-2015databook.pdf.

12 Federal Trade Commission; "Consumer Sentinel Network Data Book for January 2018- February 2019," February 2019 (accessed November 20, 2019), p. 7, at https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2018/consumer_sentinel_network_data_book_2018_0.pdf

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

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

15 United States Department of Justice, "Jamaican Citizen Admits to Participating in Lottery Scam Targeting Elderly Victims," May 25, 2017 (accessed November 20, 2019), https://www.justice.gov/usao-ndny/pr/jamaican-citizen-admits-participating-lottery-scam-targeting-elderly-victims

16 Federal Trade Commission; "Consumer Information, Online Dating Scams," accessed January 22, 2017, at https://www.consumer.ftc.gov/articles/0004-online-datingscams.

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

18 *Justice Department Coordinates Largest-even Nationwide Elder Fraud Sweep (2019, March 7).* Retrieved October 23, 2019, from https://www.justice.gov/opa/pr/justice-department-coordinates-largest-ever-nationwide-elder-fraud-sweep-0.

19 U.S. Department of Justice, "Justice Department Coordinates Largest-even Nationwide Elder Fraud Sweep," press releases, March 7, 2019 (accessed December 4, 2019), at https://www.justice.gov/opa/pr/justice-department-coordinates-largest-ever-nationwide-elder-fraud-sweep-0

20 U.S. Congress, Senate Special Committee on Aging, *Fighting Elder Fraud: Progress Made, Work to be Done*, hearings, 116th Cong., 1st sess., January 16, 2019 https://www.aging.senate.gov/imo/media/doc/SCA_Flavin_complete_01_16_19.pdf

21 Attorney General's Annual Report to Congress on Department of Justice Activities to Combat Elder Abuse and Financial Exploitation. October 18, 2018. Pg. 16-17. (accessed on December 15, 2018).

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

23 TIGTA briefing with Aging Committee, November 1, 2019.

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

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

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

27 Ibid., 14.

28 Ibid., 15.

29 Ibid, 15

30 Ibid., 10.

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

TIPS FROM THE UNITED STATES SENATE SPECIAL COMMITTEE ON AGING

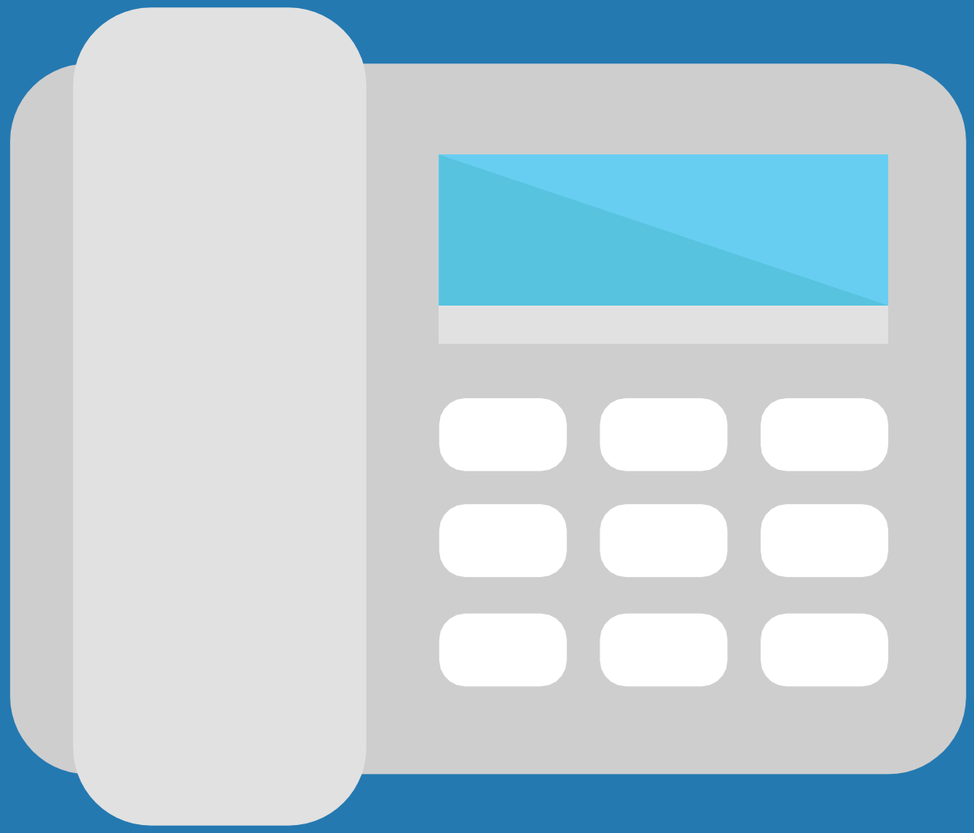
How To Avoid Phone Scams

BEWARE OF CALLERS THAT:

- Force you to make fast decisions and threaten you with police action.
- Pressure you not to tell friends and family about the call.
- Ask for personal information like Social Security or bank account numbers.

REMEMBER:

- If you receive a suspicious call asking for your personal or bank information, HANG UP IMMEDIATELY!



If you think you have been the victim of fraud, please contact the Senate Aging Committee's Fraud Hotline at 1-855-303-9470.

Notes

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

1-855-303-9470