

SENIOR INVESTOR PROTECTION INITIATIVE



DIGITAL RESOURCES

SIFMA Senior Investor Protection Toolkit is now available online!

Always have access to SIFMA's Senior Investor Protection Toolkit. View all these valuable materials available in this Toolkit, plus the additional resources below, online.

- Customizable Model Trusted Contact Authorization Form
- Video Testimonials from Unlikely Victims
- Blog Posts on the Aging Process and Cognitive Decline
- Real-Life Case Studies on Financial Exploitation Scams
- Additional Useful Databases

INTRODUCTION

Financial advisors most likely serve as the first-line of defense when protecting senior investors. One of the most common difficulties they experience in this role, however, is convincing a resistent client that they are the target of a scam, fraud or other financial exploitation attempt.

SIFMA is committed to finding solutions that help protect senior investors from financial exploitation and cognitive decline. As part of this effort, SIFMA has created this Senior Investor Protection Playbook for financial advisors. This valuable resource is a compilation of documents that explain the most common types of scams and exploitation attempts and highlights some of the key red flags associated with each of these scenarios.

The Playbook is designed to fulfill two roles. First, it will provide both financial advisors and their senior clients with information ahead of time so that they are forewarned of potential scams and armed with the information necessary to protect themselves. Second, the Playbook will assist an advisor in communicating to clients that they are being exploited by providing the advisor with prepared materials that parallel the situation in which the client currently finds themselves.

These resources come from organizations across the United States, including the federal government (the Federal Trade Commission), state securities regulators, not-for-profit organizations and universities. The goal of this Playbook is to help dedicated financial advisors, like you, educate and explain potential threats to their clients and take action when a threat is known or suspected.

For more information and to learn more about SIFMA's efforts, please visit: www.sifma.org/seniorinvestors.

Table of Contents

I.	Trusted Individuals	
	Undue Influence (WISER/SIFMA)	3
	Power of Attorney Abuse (WISER/SIFMA)	7
	Online Dating Scams (FTC)	11
	Affinity Fraud (New Mexico Securities Division)	13
II.	Imposter Fraud	
	Grandkid Scams (FTC)	17
	Tech Support Scams (FTC)	19
	"You've' Won" Scams (FTC)	21
	IRS Imposter Scams (FTC)	23
	Imposter Scams (Generally) (FTC)	25
III.	Fake Company/Service	
	Charity Fraud (FTC)	27
	Deed Theft & Foreclosure Rescue Scams (WISER/SIFMA)	29
	Disaster Fraud Awareness (Stetson University)	33
IV.	Identity Theft	
	Identity Theft & Credit Card Fraud (WISER/SIFMA)	35
	Identity Theft (FTC)	39
	Protecting your Identity (New Mexico Securities Division)	41
	Healthcare Scams (WISER/SIFMA)	43
	Healthcare Scams (FTC)	47
	Identity Theft Awareness (Stetson University)	49
V.	Exploitation Overviews	
	Senior Financial Fraud and Abuse (WISER/SIFMA)	51
	Investment Fraud Prevention (New Mexico Securities Division)	55
	Current & Common Scams in 2015 (Stetson University)	57
	Top Scams Targeting Veterans (Stetson University)	59

WISER/SIFMA

Just the Facts: Senior Financial Abuse— Undue Influence



Introduction

Senior financial abuse scams are a multi-billion dollar "industry." Studies estimate the annual financial loss nationwide to be around \$2.9 billion¹. In a recent New York State study, estimated annual losses for seniors in a subsample of New York State districts fell between \$352 million to \$1.5 billion, suggesting the national total may be substantially higher than previously estimated.² Although it can be difficult to measure the exact extent of the total financial loss, we know that these crimes are on the rise and continue to deprive seniors of their savings and assets. These figures do not account for the tens of billions spent on indirect costs for medical care, social services, and legal costs, or for the pain and suffering of the victims. Victims are not only older people, but also their families and all who provide services and financial assistance.

All seniors, regardless of income, are at risk. Financial abuse may be perpetrated by anyone—a professional con artist, a paid caregiver, a stranger or casual acquaintance, or even a son, daughter, or other family member.

The following factors contribute to the prevalence of senior financial abuse:

- A high percentage of seniors live alone and may be more vulnerable to scams.
- Seniors may be trusting and readily believe the sales "pitches" they hear.
- The population of seniors is increasing, providing a continuous source of wealth for financial abusers.

WHAT IS UNDUE INFLUENCE?

Undue influence is the "persuasion, pressure, or influence short of actual force, that so overpowers the dominated party's free will or judgment that he or she cannot act intelligently or voluntarily."

Education and awareness are two key strategies to preventing and responding to elder financial abuse. This brief describes a type of abuse, called undue influence, and provides resources to keep seniors from becoming victims.

© Women's Institute for a Secure Retirement/SIFMA, 2016

Undue Influence

Undue influence is a critical part of any type of senior abuse – financial, physical, or sexual. Some seniors are more likely to be vulnerable to undue influence because they are more trusting in nature or have a reason to be dependent on someone else. Sometimes, because of a disability, a senior must rely on someone else to help with everyday activities. Other times, the senior may be isolated, depressed or grieving, and need someone for emotional support.

How You Can Recognize Undue Influence

Undue influence is often the cause of other types of financial abuse and shares many of the same indicators. Signs include:

- Missing checks or property.
- Unusual activity in bank accounts.
- Eviction notices or lack of utilities that should be provided by the senior's income.
- Placement, care, or living conditions that do not match the senior's financial ability to pay.
- A recent acquaintance or caregiver who expresses an unusual affection for the senior and may have moved into the senior's home or apartment.
- A caregiver who shows unusual interest in the senior's financial arrangements.
- A caregiver who promises lifelong care, or threatens to leave the senior, in exchange for the senior's property.

Since undue influence involves one person wholly taking advantage of someone unable to defend herself or himself, many consider it a type of domestic violence.

Similarities to domestic violence include:

- The victim and the abuser have an ongoing relationship that allows the abuse to occur.
- The abuser may 'charm' the victim, to gain control.
- The abuser isolates the victim and creates dependency on the abuser or the abuser provides inadequate nutrition, withholds medication, or deprives the victim of sleep.



How You Can Help Stop Undue Influence

Someone close to the victim, either a relative or close friend, often exercises undue influence. Many cases of undue influence go undocumented because seniors hide or minimize the abuse and protect the abuser in order to avoid conflicts within their family. Also, dishonest guardians, conservators, and those given Power of Attorney can exercise undue influence. To help determine if the senior is being unduly influenced:

¹ The MetLife Mature Market Institute. The MetLife Study of Elder Financial Abuse. June 2011.

² New York State Office of Children and Family Service. The New York State Cost of Financial Exploitation Study June 15, 2016

Explore the relationship between the senior and the suspected perpetrator

- How much time does the suspected perpetrator spend with the senior?
- Is the alleged perpetrator a recent acquaintance or family member?
- Are there signs that the alledged perpetrator has financial, mental health or substance abuse problems?
- Does the senior have the mental capacity and ability to make financial decisions?

Assess the total situation

- Has the senior become socially withdrawn or isolated?
- Have the living conditions of the senior deteriorated?
- Are basic amenities lacking from the house?

Document discrepancies

- Do the check signatures look fraudulent?
- Are funds being diverted to accounts the senior does not solely control?
- Is the alleged perpetrator giving unclear, contradictory, or elusive responses about the senior's situation?



www.ncea.acl.gov

If you suspect wrongdoing, immediately notify Adult Protective Services and file a report with the local police department. You may also contact the prosecuting attorney (or district attorney) in your area. **You do not need to prove that abuse is occurring; it is up to the professionals to investigate the suspicions.** Law enforcement will look for evidence of the suspect undermining the victim's confidence, and manipulating and lying to the victim.

Call the police or 9-1-1 immediately if someone you know is in immediate, life-threatening danger.

ADDITIONAL HELPFUL RESOURCES -

Many public agencies are involved in preventing and detecting senior abuse and in prosecuting those who commit it. Many organizations are also dedicated to educating seniors on these topics:

- National Center on Elder Abuse State Resources: Helplines, Hotlines and Information.
- **National Center for Victims of Crime** www.victimsofcrime.org

Financial Crime Resource CenterHelps victims of financial crime recover their assets and recover control of their lives.

- * Federal Trade Commission www.ftc.gov
- Protects consumers from unfair, deceptive and fraudulent business practices.
- * Financial Fraud Enforcement Task Force www.stopfraud.gov
 A coalition of federal, state, and local law enforcement that investigates and prosecutes financial fraud.
- * Postal Inspection Service www.postalinspectors.uspis.gov Investigates domestic and international fraud which uses the U.S. Mail.
- The Securities and Exchange Commission (SEC)
 Investigates securities and investment fraud.
 1-800-732-0330
- U.S. Administration on Aging

 In partnership with the National Association of Area Agencies on Aging,
 Operates the Eldercare Locator to help individuals find local caregiving services and resources.

ADMINISTRATION ON AGING RESOURCE CENTERS

partner to provide valuable information to seniors, caregivers, families and communities across the nation.

National Resource Center on Women and Retirement Planning

National Resource Center on Women Retirement Planning The Women's Institute for a Secure Retirement (WISER), in partnership with the Administration on Aging, operates the National Resource Center on Women and Retirement Planning to provide user-friendly financial education and retirement planning tools for low-income women, women of color, and women with limited English speaking proficiency. WISER's mission is to inform women about the issues that affect their long-term financial security and to stress the

importance of taking an active role in planning for retirement. The Center specially tailors educational financial tools and information to meet the needs of the target population. Through the Center's one stop gateway, women have access to comprehensive, easily understood information that allows them opportunities to plan for income during retirement and to plan for long-term care

as they need it.

1140 19th Street, NW, Suite 550 Washington, DC 20036 (202) 393-5452

www.wiserwomen.org



New York

120 Broadway, 35th Floor New York, N.Y. 10271 212.313.1200

Washington, D.C.

1101 New York Avenue, NW 8th Floor Washington, D.C. 20005 202.962.7300

www.sifma.org



The Securities Industry and Financial Markets Association (SIFMA)

The Securities Industry and Financial Markets Association (SIFMA) is the voice of the nation's securities industry, bringing together the shared interests of hundreds of broker-dealers, banks and asset managers. SIFMA advocates for effective and resilient capital markets. WISER and SIFMA are proud to partner together to raise awareness about the problem of elder financial fraud and abuse, as well as provide education and resources to help prevent these crimes from occurring.

- © Women's Institute for a Secure Retirement/SIFMA, 2016 -

WISER/SIFMA Just the Facts: Senior Financial Abuse: Power of Attorney Abuse



Introduction

Senior financial abuse scams are a multi-billion dollar "industry." Studies estimate the annual financial loss nationwide to be around \$2.9 billion¹. In a recent New York State study, estimated annual losses for seniors in a subsample of New York State districts fell between \$352 million to \$1.5 billion, suggesting the national total may be substantially higher than previously estimated.² Although it can be difficult to measure the exact extent of the total financial loss, we know that these crimes are on the rise and continue to deprive seniors of their savings and assets. These figures do not account for the tens of billions spent on indirect costs for medical care, social services, and legal costs, or for the pain and suffering of the victims. Victims are not only older people, but also their families and all who provide services and financial assistance.

All seniors, regardless of income, are at risk. Financial abuse may be perpetrated by anyone—a professional con artist, a paid caregiver, a stranger or casual acquaintance, or even a son, daughter, or other family member.

The following factors contribute to the prevalence of senior financial abuse:

- A high percentage of seniors live alone and may be more vulnerable to scams.
- Seniors may be trusting and readily believe the sales "pitches" they hear.
- The population of seniors is increasing, providing a continuous source of wealth for financial abusers.

Education and awareness are two key strategies to preventing and responding to elder financial abuse. This fact sheet looks at power of attorney abuse and provides resources to keep seniors from falling victim to these financial traps.

SOME PEOPLE
MAY USE POWER
OF ATTORNEY
MALICIOUSLY,
CAUSING A SENIOR
TO LOSE HER HOME,
ASSETS, AND
OTHER PROPERTY.

Power of Attorney Abuse

Granting power of attorney (POA) to someone is a significant step. Having power of attorney over someone means having the right to make legal decisions for that person. Some people can use this power maliciously, causing a senior to lose her home, assets, and other property.

In the hands of a trustworthy person, POA is an important tool to manage the finances of a senior who is temporarily or permanently unable to handle his or her own affairs.

The Different Types of Power of Attorney

1. General

Unlimited in scope or duration, and permits the agent to act as the person's legal representative until it is revoked.

2. Special or Limited

Gives the agent power over specific situations when the person is unavailable or unable to take action because of other commitments or health reasons.

3. Durable

Remains in effect when the person becomes incapacitated.

4. Springing

Does not become effective until a condition stated in the document is met.

How You Can Help Stop Power of Attorney Abuse

To make sure someone who has or is seeking to gain power of attorney does not victmize the senior, conduct a thorough investigation.

Determine the relationship between the agent and the senior. Is the agent a stranger to the senior? Close relative? Friend?



- Interview the senior. Are there signs of confusion or mental incapacity?
- Review financial records for transactions that benefit the agent rather than the senior.

WHAT IS POWER OF

ATTORNEY?

Power of Attorney (POA) is

a legal document that gives

authority for one person

to act for another person

in some or all legal and

financial matters.

If there are any signs of wrongdoing, immediately file a report with the police department where the crime was located. Contact the guardian or conservator to revoke the POA. And contact the county attorney who may be able to both prosecute the agent and sue for restitution.

¹ The MetLife Mature Market Institute. The MetLife Study of Elder Financial Abuse. June 2011.

New York State Office of Children and Family Service. The New York State Cost of Financial Exploitation Study June 15, 2016

Signs of Power of Attorney Abuse

There are different indicators of Power of Attorney abuse. The signs can come from the senior, the agent, or from the senior's home.

General Things To Look Out For

Documents stating the onset of a senior's incapacity prior to the signing of a POA

Unusual or erratic banking activity

Lack of amenities even though the senior could afford them

Red Flags: Power of Attorney Agent

- The agent is vague or evasive about financial arrangements
- Purchases made by the agent are not on the senior's behalf
- The agent's decisions do not seem to be in the senior's best interests

Red Flags: Senior

- The senior and/or residence is unkempt even though care was arranged
- The senior is forced to sell property
- The senior is placed in a facility well below their ability to pay



ADDITIONAL HELPFUL RESOURCES

Many public agencies are involved in preventing and detecting senior abuse and in prosecuting those who commit it. Many organizations are also dedicated to educating seniors on these topics:

National Center on Elder Abuse

www.ncea.acl.gov

Provides state resources: helplines, hotlines and information.

National Academy of Elder Law Attorneys

www.naela.org

Find attorneys specializing in Elder and Special Needs law.

Federal Trade Commission

www.ftc.gov

Protects consumers from unfair, deceptive and fraudulent business practices.

Federal Crimes Enforcement Network

www.stopfraud.gov

Financial Fraud Enforcement Task Force Investigates suspected financial fraud

American Bar Association Commission on Law and Aging

www.abanet.org

Lists statewide resources to help older adults with legal issues

The Securities and Exchange Commission Investigates securities frauds

www.investor.gov

U.S. Administration on Aging

www.eldercare.gov 1-800-677-1116

In partnership with the National Association of Area Agencies on Aging,

operates the Eldercare Locator to help individuals find local caregiving services and resources.

ADMINISTRATION ON AGING RESOURCE CENTERS

partner to provide valuable information to seniors, caregivers, families and communities across the nation.

National Resource Center on Women and Retirement Planning

National Resource Center on Women Retirement Planning The Women's Institute for a Secure Retirement (WISER), in partnership with the Administration on Aging, operates the National Resource Center on Women and Retirement Planning to provide user-friendly financial education and retirement planning tools for low-income women, women of color, and women with limited English speaking proficiency. WISER's mission is to inform women about the issues that affect their long-term financial security and to stress the

importance of taking an active role in planning for retirement. The Center specially tailors educational financial tools and information to meet the needs of the target population. Through the Center's one stop gateway, women have access to comprehensive, easily understood information that allows them opportunities to plan

for income during retirement and to plan for long-term care as they need it.

1140 19th Street, NW, Suite 550 Washington, DC 20036 (202) 393-5452 www.wiserwomen.org



New York

120 Broadway, 35th Floor New York, N.Y. 10271 212.313.1200

Washington, D.C.

1101 New York Avenue, NW 8th Floor Washington, D.C. 20005 202.962.7300

www.sifma.org



The Securities Industry and Financial Markets Association (SIFMA)

The Securities Industry and Financial Markets Association (SIFMA) is the voice of the nation's securities industry, bringing together the shared interests of hundreds of broker-dealers, banks and asset managers. SIFMA advocates for effective and resilient capital markets. WISER and SIFMA are proud to partner together to raise awareness about the problem of elder financial fraud and abuse, as well as provide education and resources to help prevent these crimes from occurring.

© Women's Institute for a Secure Retirement/SIFMA, 2016 -



Online Dating Scams

Here's how they work:

You meet someone special on a dating website. Soon he wants to move off the dating site to email or phone calls. He tells you he loves you, but he lives far away — maybe for business, or because he's in the military.

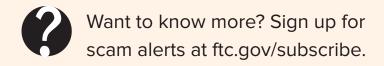
Then he asks for money. He might say it's for a plane ticket to visit you. Or emergency surgery. Or something else urgent.

Scammers, both male and female, make fake dating profiles, sometimes using photos of other people — even stolen pictures of real military personnel. They build relationships — some even fake wedding plans — before they disappear with your money.

Here's what you can do:

- 1. Stop. Don't send money. Never wire money, put money on a prepaid debit card, or send cash to an online love interest. You won't get it back.
- 2. Pass this information on to a friend. You may not have gotten one of these calls, but chances are you know someone who will get one if they haven't already.







Please Report Scams

If you spot a scam, please report it to the Federal Trade Commission.

- Call the FTC at 1-877-FTC-HELP (1-877-382-4357) or TTY 1-866-653-4261
- Go online: ftc.gov/complaint

Your complaint can help protect other people.

By filing a complaint, you can help the FTC's investigators identify the imposters and stop them before they can get someone's hard-earned money. It really makes a difference.

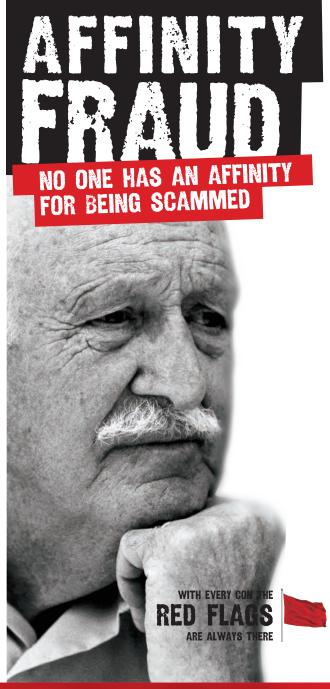








12





Regulation and Licensing

Securities Division

2550 Cerrillos Rd Santa Fe, NM, 87505

1.800.704.5533 www.redflagsnm.com

> **New Mexico Regulation and Licensing Securities Division**

> > redflagsnm.com | 1.800.704.5533

In a world of increasing complexity, many people feel the need for a shorthand way of knowing whom to trust. This is especially true when it comes to investing money. Unfamiliar with how our financial markets work, many people don't know how to research an investment or its seller thoroughly. Many fall prey to affinity group fraud, in which a con artist claims to be a member of the same ethnic, religious, career or community-based group.

AFFINITY FRAUD IS A CRIME. IN RECENT YEARS IT HAS CAUSED HUNDREDS OF HONORABLE PEOPLE TO LOSE MILLIONS OF DOLLARS OF THEIR HARD-EARNED MONEY TO INDIVIDUALS THEY BELIEVED COULD BE TRUSTED

WHOM TO TRUST

IN A WORLD OF INCREASING COMPLEXITY, MANY PEOPLE FEEL THE NEED FOR A SHORTHAND WAY OF KNOWING WHOM TO TRUST

This is especially true when it comes to investing money. Unfamiliar with how our financial markets work, many people don't know how to research an investment or its seller thoroughly. Many fall prey to affinity group fraud, in which a con artist claims to be a member of the same ethnic, religious, career or community-based group.

"You can trust me" says the con artist, "because I'm like you. We share the same background and interests. And I can help you make money."

Many new arrivals to America are seen by swindlers as ripe for the picking. Sometimes, they are isolated from the larger community, their access to information limited by language and other barriers.

Some members of long-established minority groups have accumulated savings and achieved a certain standard of living through years of hard work. Often, they want to give back to the community in order to help others like themselves. However, such inclinations often make these groups easy prey for con artists who, despite sharing the same ethnicity or culture, are motivated by greed.

Religious affinity group swindlers are found across all denominations. Consumers have complained about fraud and abuse by "born again" financial planners, con artists claiming church endorsements, and givers of "divinely inspired" investment advice.

Many of these scams are based on dire predictions of imminent financial and social chaos, such as a sharp drop in the stock market. Specialized media outlets - religious-oriented magazines, newspapers, radio stations and cable television outlets - make it easy for a con artist to target the faithful.

HOW THEY DO IT AND GET AWAY WITH IT

Another equally effective pitch - if the con artist is not a member of the group - is to lull members into a misplaced trust by first selling to a few prominent members and giving them a quick return on their money. Using their names, the con artist pitches the scam to the rest of the group. Once they have gained your confidence, the individual's skepticism melts away and another sale occurs.

Even after the investor recognizes the scam for what it is, he often doesn't notify authorities. Instead, he tries to solve problems within the group. Swindlers who prey on minorities play the loyalty angle for all it is worth.

It is usually difficult to catch perpetrators of affinity fraud scams because victims are embarrassed to admit that they were conned and reluctant to turn in "one of their own." Even when victims realize they have been deceived, rather than notifying the authorities, they often keep quiet or try to work things out within the group. Con artists understand and exploit this reluctance to report the fraud. As a result, good people lose their hard-earned savings and sense of trust, the authorities cannot act without the cooperation of victims - and the fraudsters keep the money, moving on to repeat the scam with other groups in new places.

Don't get taken. Investigate before you invest. Notify authorities if you think you've been scammed.

HOW THE FAITHFUL CAN AVOID SCAMS

BE WARY OF ANY INVESTMENT THAT SEEMS CLOSELY TIED TO A PARTICULAR RELIGIOUS BELIEF

It makes little sense that an investment opportunity would be available only to members of a specific church or faith. Many religious scriptures warn of those who would exploit faith for personal enrichment.

BE CAUTIOUS

if the promoter of an investment opportunity tries to capitalize on connections or leadership within a religious group. The success of the investment is unlikely to be linked to the promoter's inside contacts. Exercise the same caution and skepticism that you would with any other investment.

BEWARE OF A NEW MEMBER OF YOUR CHURCH WHO SPRINGS UP OUT OF NOWHERE WITH A SURE-FIRE INVESTMENT SCHEME

Some con artists will waste no time ingratiating themselves within a religious circle. Find out about their background, if any, within the church.

IGNORE CLAIMS THAT RELIGION-BASED INVESTMENTS AREN'T REGULATED

Almost all investments, including church bonds, are regulated by state and federal securities or commodities laws.

CHECK OUT THE PROMOTER AND THE INVESTMENT

Contact the New Mexico Securities Division at 1-800-704-5533 to find out if they are registered in the State of New Mexico. Your local Better Business Bureau may have records of complaints about the promoter.

DON'T GIVE A BREAK TO A SWINDLER WHO HIDES BEHIND RELIGION

Don't be victimized for a second time by letting an investment scammer off the hook. He might take the opportunity to take advantage of new victims elsewhere.

PROTECT YOURSELF

THE TIGHT-KNIT STRUCTURE OF MANY RELIGIOUS, COMMUNITY AND SOCIAL GROUPS IS A PERFECT ENVIRONMENT FOR THE CON ARTIST

BEWARE OF THE USE OF NAMES OR TESTIMONIALS FROM OTHER GROUP MEMBERS

Scam artists frequently pay high returns to early investors with money generated from later investors. As a result, early investors might be wildly enthusiastic about a scheme that collapses once you've invested.

GET PROOF IN WRITING

Obtain a prospectus or other form of written information that details the risks in the investment, as well as procedures for getting your money out.

ASK FOR PROFESSIONAL ADVICE FROM A NEUTRAL OUTSIDE EXPERT

Consult with someone not in your group - an accountant, attorney, or financial planner - to evaluate the investment.

CONTACT THE NEW MEXICO SECURITIES DIVISION

Ask for information about the firm and the person selling the investment, including whether they're registered. Any investment and the person selling the investment must both be registered with the New Mexico Securities Division.

PROTECT YOURSELF

The New Mexico Securities Division strongly urges every New Mexican, particularly seniors, to investigate before they invest. Check out the investment opportunity and the person selling you the investment before you give them any of your money. Always ask for written information about investment opportunities and keep this information in your permanent records.



Grandkid Scams

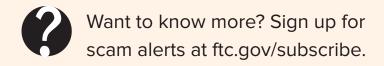
Here's how they work:

You get a call: "Grandma, I need money for bail." Or money for a medical bill. Or some other kind of trouble. The caller says it's urgent — and tells you to keep it a secret.

But is the caller who you think it is? Scammers are good at pretending to be someone they're not. They can be convincing: sometimes using information from social networking sites, or hacking into your loved one's email account, to make it seem more real. And they'll pressure you to send money before you have time to think.

Here's what you can do:

- 1. Stop. Check it out. Look up your grandkid's phone number yourself, or call another family member.
- 2. Pass this information on to a friend. You may not have gotten one of these calls, but chances are you know someone who will get one if they haven't already.





Please Report Scams

If you spot a scam, please report it to the Federal Trade Commission.

- Call the FTC at 1-877-FTC-HELP (1-877-382-4357) or TTY 1-866-653-4261
- Go online: ftc.gov/complaint

Your complaint can help protect other people. By filing a complaint, you can help the FTC's investigators identify the imposters and stop them before they can get someone's hard-earned money. It really makes a difference.









18



Tech Support Scams

Here's how they work:

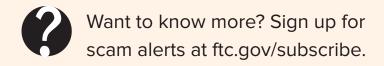
You get a call from someone who says he's a computer technician. He might say he's from a well-known company like Microsoft, or maybe your internet service provider. He tells you there are viruses or other malware on your computer. He says you'll have to give him remote access to your computer or buy new software to fix it.

But is the caller who he says he is? Judging by the complaints to the Federal Trade Commission, no. These scammers might want to sell you useless services, steal your credit card number, or get access to your computer to install malware, which could then let them see everything on your computer.

Here's what you can do:

- **1. Hang up.** Never give control of your computer or your credit card information to someone who calls you out of the blue.
- 2. Pass this information on to a friend. You might know these calls are fakes, but chances are you know someone who doesn't.







Please Report Scams

If you spot a scam, please report it to the Federal Trade Commission.

- Call the FTC at 1-877-FTC-HELP (1-877-382-4357) or TTY 1-866-653-4261
- Go online: ftc.gov/complaint

Your complaint can help protect other people.

By filing a complaint, you can help the FTC's investigators identify the imposters and stop them before they can get someone's hard-earned money. It really makes a difference.









20



"You've Won" Scams

Here's how they work:

You get a card, a call, or an email telling you that you won! Maybe it's a trip or a prize, a lottery or a sweepstakes. The person calling is so excited and can't wait for you to get your winnings.

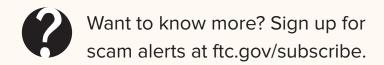
But here's what happens next: they tell you there's a fee, some taxes, or customs duties to pay. And then they ask for your credit card number or bank account information, or they ask you to wire money.

Either way, you lose money instead of winning it. You don't ever get that big prize. Instead, you get more requests for money, and more promises that you won big.

Here's what you can do:

- 1. Keep your money and your information to yourself. Never share your financial information with someone who contacts you and claims to need it. And never wire money to anyone who asks you to.
- 2. Pass this information on to a friend. You probably throw away these kinds of scams or hang up when you get these calls. But you probably know someone who could use a friendly reminder.







Please Report Scams

If you spot a scam, please report it to the Federal Trade Commission.

- Call the FTC at 1-877-FTC-HELP (1-877-382-4357) or TTY 1-866-653-4261
- Go online: ftc.gov/complaint

Your complaint can help protect other people. By filing a complaint, you can help the FTC's investigators identify the scammers and stop them before they can get someone's hard-earned money. It really makes a difference.





22



IRS Imposter Scams

Here's how they work:

You get a call from someone who says she's from the IRS. She says that you owe back taxes. She threatens to sue you, arrest or deport you, or revoke your license if you don't pay right away. She tells you to put money on a prepaid debit card and give her the card numbers.

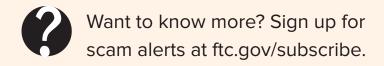
The caller may know some of your Social Security number. And your caller ID might show a Washington, DC area code. But is it really the IRS calling?

No. The real IRS won't ask you to pay with prepaid debit cards or wire transfers. They also won't ask for a credit card over the phone. And when the IRS first contacts you about unpaid taxes, they do it by mail, not by phone. And caller IDs can be faked.

Here's what you can do:

- 1. Stop. Don't wire money or pay with a prepaid debit card. Once you send it, the money is gone. If you have tax questions, go to irs.gov or call the IRS at 800-829-1040.
- 2. Pass this information on to a friend. You may not have gotten one of these calls, but the chances are you know someone who has.







Please Report Scams

If you spot a scam, please report it to the Federal Trade Commission.

- Call the FTC at 1-877-FTC-HELP (1-877-382-4357) or TTY 1-866-653-4261
- Go online: ftc.gov/complaint

Your complaint can help protect other people.

By filing a complaint, you can help the FTC's investigators identify the imposters and stop them before they can get someone's hard-earned money. It really makes a difference.











Imposter Scams

Here's how they work:

You get a call or an email. It might say you've won a prize. It might seem to come from a government official. Maybe it seems to be from someone you know – your grandchild, a relative or a friend. Or maybe it's from someone you *feel* like you know, but you haven't met in person – say, a person you met online who you've been writing to.

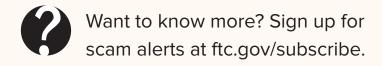
Whatever the story, the request is the same: wire money to pay taxes or fees, or to help someone you care about.

But is the person who you think it is? Is there an emergency or a prize? Judging by the complaints to the Federal Trade Commission (FTC), the answer is no. The person calling you is pretending to be someone else.

Here's what you can do:

- 1. Stop. Check it out before you wire money to anyone. Call the person, the government agency, or someone else you trust. Get the real story. Then decide what to do. No government agency will ever ask you to wire money.
- 2. Pass this information on to a friend. You may not have gotten one of these calls or emails, but the chances are you know someone who has.







Please Report Scams

If you spot a scam, please report it to the Federal Trade Commission.

- Call the FTC at 1-877-FTC-HELP (1-877-382-4357) or TTY 1-866-653-4261
- Go online: ftc.gov/complaint

Your complaint can help protect other people.

By filing a complaint, you can help the FTC's investigators identify the imposters and stop them before they can get someone's hard-earned money. It really makes a difference.









26



Charity Fraud

Here's how it works:

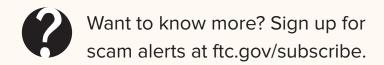
Someone contacts you asking for a donation to their charity. It sounds like a group you've heard of, it seems real, and you want to help.

How can you tell what charity is legitimate and what's a scam? Scammers want your money quickly. Charity scammers often pressure you to donate right away. They might ask for cash, and might even offer to send a courier or ask you to wire money. Scammers often refuse to send you information about the charity, give you details, or tell you how the money will be used. They might even thank you for a pledge you don't remember making.

Here's what you can do:

- 1. Take your time. Tell callers to send you information by mail. For requests you get in the mail, do your research. Is it a real group? What percentage of your donation goes to the charity? Is your donation tax-deductible? How do they want you to pay? Rule out anyone who asks you to send cash or wire money. Chances are, that's a scam.
- 2. Pass this information on to a friend. It's likely that nearly everyone you know gets charity solicitations. This information could help someone else spot a possible scam.







Please Report Scams

If you spot a scam, please report it to the Federal Trade Commission.

- Call the FTC at 1-877-FTC-HELP (1-877-382-4357) or TTY 1-866-653-4261
- Go online: ftc.gov/complaint

Your complaint can help protect other people.

By filing a complaint, you can help the FTC's investigators identify scammers and stop them before they can get someone's hard-earned money. It really makes a difference.





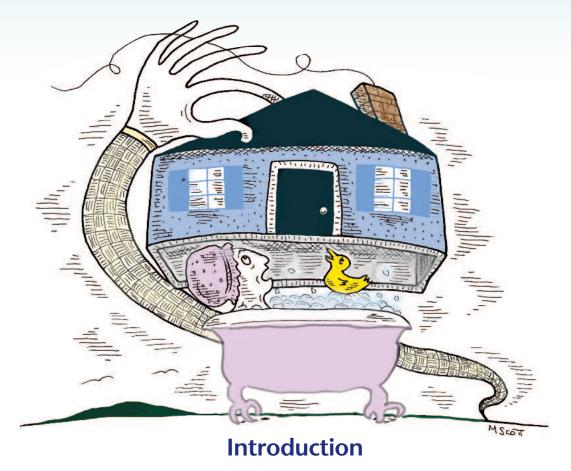




28

WISER/SIFMA

Just the Facts: DEED THEFT & FORECLOSURE RESCUE SCAMS



Senior financial abuse scams are a multi-billion dollar "industry." Studies estimate the annual financial loss nationwide to be around \$2.9 billion¹. In a recent New York State study, estimated annual losses for seniors in a subsample of New York State districts fell between \$352 million to \$1.5 billion, suggesting the national total may be substantially higher than previously estimated.² Although it can be difficult to measure the exact extent of the total financial loss, we know that these crimes are on the rise and continue to deprive seniors of their savings and assets. These figures do not account for the tens of billions spent on indirect costs for medical care, social services, and legal costs, or for the pain and suffering of the victims. Victims are not only older people, but also their families and all who provide services and financial assistance.

All seniors, regardless of income, are at risk. Financial abuse may be perpetrated by anyone—a professional con artist, a paid caregiver, a stranger or casual acquaintance, or even a son, daughter, or other family member.

The following factors contribute to the prevalence of senior financial abuse:

- A high percentage of seniors live alone and may be more vulnerable to scams.
- Seniors may be trusting and readily believe the sales "pitches" they hear.
- The population of seniors is increasing, providing a continuous source of wealth for financial abusers.

Education and awareness are two key strategies to preventing and responding to elder financial abuse. This fact sheet looks at deed theft and foreclosure rescue scams and provides resources to keep seniors from becoming victims.

DEED THEFT AND
FORECLOSURE RESCUE
SCAMS HAVE BEEN
ON THE RISE SINCE THE
2008 HOUSING CRISIS.

Deed Theft and Foreclosure Rescue Scams

Foreclosure rescue scams and deed theft are tricks con artists use to steal property from unsuspecting seniors. Feeding off the fear of losing their homes, many seniors believe these scammers out of desperation and are

WHAT ARE DEED THEFTS?

Deed thefts are the fraudulent transfer of property to another person, in which that person gains legal right to the property.

WHAT ARE FORECLOSURE RESCUE SCAMS?

These scams trick senior homeowners out of their money by promising to help with their mortgage payments. betrayed by their own trusting nature. Unfortunately, these types of scams are also becoming more prevalent.

In a foreclosure scam, the scammer contacts the distressed homeowner, making an offer to save the home from foreclosure. The scammer vanishes after draining as much money out of the victim as possible, through fees or charges. Sometimes, the scammer also tricks the property owner into handing over the property by having the owner sign for a "new" loan. This crosses over into deed theft.

Deed theft typically involves either tricking or coercing the owner of a property into signing a quitclaim deed, a document that transfers ownership of a senior's property over to the scammer. However, deed theft may occur without the homeowner even knowing in instances where the scammer files a phony deed.

How To Tell If A Broker Is Legitimate

There are many ways to tell if a broker or company is legitimate or not. Be suspicious and avoid brokers or companies that do any of the following:

- Call themselves "mortgage consultants" or the company a "foreclosure service".
- Offer a loan modification for a fee or ask for fees in advance.
- Make verbal promises and lofty claims. (If it's too good to be true, it probably is!)
- Give advice to break contact with the senior's attorney or family.
- Have an unclear document process with irregularities such as lack of a notary.
- Try to get the victim to transfer ownership of the property (deed theft).

Red Flags: Deed Theft

Foreclosure rescue scams and deed theft are related, with many overlapping indicators. However, deed theft is more likely to be done by a relative or close friend of the victim.

Look for these signs to spot possible deed theft:

- Mental confusion on the part of the signer that predated the signing of the deed. Deeds signed by persons not mentally competent are likely not valid.
- Suspicion that the senior signing over their property was defrauded, coerced, unduly influenced or not particularly aware of the transaction.
- No notary being present when the senior signed the quitclaim deed.
- Future care was promised in exchange for the signing over of the property.

How You Can Help Stop Deed Theft and Foreclosure Scams

If a senior has been victimized in a deed theft or foreclosure scam, conduct a thorough review.



Investigate:

- What was the relationship between the senior and possible scammer?
- Was the senior mentally capable of understanding the transaction?
- Is there paperwork documenting the transaction?
- Did the salesperson claim to have special designations such as a Certified Senior Advisor?

If there are any signs of wrongdoing, immediately file a report with the police department where the crime was located. Sometimes the threat of prosecution will convince the perpetrator to either return the property or stop ongoing theft. Also, determine if the senior has signed a "Life Estate," a legal document that protects a senior's right to live on the property until death if the property is handed over to a relative.

ADDITIONAL HELPFUL RESOURCES

Many public agencies are involved in preventing and detecting senior abuse and in prosecuting those who commit it. Many organizations are also dedicated to educating seniors on these topics:

National Center on Elder Abuse
State Resources: Helplines, Hotline and Information

www.ncea.acl.gov

- * Consumer Financial Protection Bureau www.consumerfinance.gov/older-americans
 Provides resources to help protect seniors' financial assets.
- Federal Trade Commission
 Protects consumers from unfair, deceptive and fraudulent business practices.
- W.S. Department of Housing and Urban Development (HUD) www.hud.gov or 1-800-225-5342
 Resources for homeowners, including how to recognize and avoid scams
- * Homeownership Preservation Foundation 1-888-995-HOPE

 Nonprofit operates toll-free hotline 24/7 with free, bilingual, personal assistance to help avoid foreclosure.

¹ The MetLife Mature Market Institute. The MetLife Study of Elder Financial Abuse. June 2011.

² New York State Office of Children and Family Service. The New York State Cost of Financial Exploitation Study June 15, 2016

ADMINISTRATION ON AGING RESOURCE CENTERS

partner to provide valuable information to seniors, caregivers, families and communities across the nation.

National Resource Center on Women and Retirement Planning

National Resource Center on Women Retirement Planning The Women's Institute for a Secure Retirement (WISER), in partnership with the Administration on Aging, operates the National Resource Center on Women and Retirement Planning to provide user-friendly financial education and retirement planning tools for low-income women, women of color, and women with limited English speaking proficiency. WISER's mission is to inform women about the issues that affect their long-term financial security and to stress the

importance of taking an active role in planning for retirement. The Center specially tailors educational financial tools and information to meet the needs of the target population. Through the Center's one stop gateway, women have access to comprehensive, easily understood information that allows them opportunities to plan

for income during retirement and to plan for long-term care as they need it.

1140 19th Street, NW, Suite 550 Washington, DC 20036 (202) 393-5452 www.wiserwomen.org



New York

120 Broadway, 35th Floor New York, N.Y. 10271 212.313.1200

Washington, D.C.

1101 New York Avenue, NW 8th Floor Washington, D.C. 20005 202.962.7300

www.sifma.org



The Securities Industry and Financial Markets Association (SIFMA)

The Securities Industry and Financial Markets Association (SIFMA) is the voice of the nation's securities industry, bringing together the shared interests of hundreds of broker-dealers, banks and asset managers. SIFMA advocates for effective and resilient capital markets. WISER and SIFMA are proud to partner together to raise awareness about the problem of elder financial fraud and abuse, as well as provide education and resources to help prevent these crimes from occurring.

- © Women's Institute for a Secure Retirement/SIFMA, 2016 -

Elder Consumer Protection Program

The Elder Consumer Protection Program at Stetson University College of Law's Center for Excellence in Elder Law is an educational and information resource on general and legal matters regarding elder consumer protection and awareness. The program, which is supported by state funding, offers assorted materials and various services that provide and promote general knowledge, public awareness and assistance, and professional development and training.

The information contained herein is intended only as a brief overview on matters of general interest. It is not offered as legal advice, is not a definite statement of law, and is not a complete analysis of the area of law.

The applicability of law to a particular matter requires an exhaustive examination of the specific facts with the appropriate laws. If you have a specific legal issue or legal concern, you should always consult with an attorney for detailed legal advice.





ELDER CONSUMER PROTECTION PROGRAM

CENTER FOR EXCELLENCE IN ELDER LAW

1401 61st Street South Gulfport, Florida 33707

Phone: (727) 562-7888 **Fax:** (727) 345-1838

E-mail: ecpp@law.stetson.edu

Web: www.stetson.edu/law/elderconsumers

Twitter: @StetsonLawECPP

STETSONLAW

STETSON UNIVERSITY

Center for Excellence in Elder Law

ACCESS AND JUSTICE FOR ALL®

© 2015 Stetson University College of Law. All Rights Reserved.

OH GAUDIL D. 1

Disaster Fraud Awareness

Price Gouging

Home Repair Fraud

Charity Fraud





Center for Excellence in Elder Law

ACCESS AND JUSTICE FOR ALL®

Price Gouging

Price Gouging occurs when someone, during a declared state of emergency, charges unreasonable prices in the sale or rental of:

- Essential Goods (such as water, fuel, batteries, food, lodging, lumber, or generators); or
- Essential Services (such as tree services, debris removal, or damaged property repair).

Help Protect Yourself

- ⇒ Plan ahead and be prepared
- ⇒ Always keep emergency items on hand (e.g., drinking water, non-perishable food, necessary medications, candles, flashlights, portable radio, batteries).
- \Rightarrow Shop Around and compare prices.
- \Rightarrow Never pay with cash.
- ⇒ Maintain detailed records of any purchases and transactions
- ⇒ Get a specific and detailed receipt

Suspect Something?

Contact:

Florida Attorney General's Fraud Hotline

By Telephone: 1-866-966-7226 Online: www.myfloridalegal.com



Home Repair Fraud

Home Repair Fraud occurs when someone:

- Makes unnecessary repairs;
- Charges inflated prices;
- Performs repairs without having the necessary or proper qualifications;
- Uses inferior materials; or
- Collects advance payment for work that is never completed

Help Protect Yourself

- ⇒ Require a detailed written estimate.
- ⇒ Obtain at least two different estimates.
- ⇒ Confirm and verify licensing and insurance.
- ⇒ Ask for and check references.
- ⇒ Avoid door-to-door and unsolicited sales.
- \Rightarrow Never pay with cash
- ⇒ Pay only when the work is completed and finished to your satisfaction.
- ⇒ Get a specific and detailed receipt.
- ⇒ Require all warranties or guarantees to be provided in writing.

Suspect Something?

Contact:

Florida Department of Business and Professional Regulation

By Telephone: 1-850-487-1395 Online: www.myfloridalicense.com

Florida Department of Agriculture and Consumer Services

By Telephone: 1-800-HELP-FLA (435-1352)

Online: www.800helpfla.com

Charity Fraud

Charity Fraud occurs when someone:

- Misuses or misappropriates funds donated to a legitimate charity; or
- Solicits donations for an illegitimate or unregistered charity.

Help Protect Yourself

- ⇒ Only donate to well known, established charities. Be suspicious of charities arising quickly in connection with a disaster or event.
- ⇒ Beware of intimidation, emotional appeals, and high-pressure tactics.
- ⇒ Ask for specific detailed written information regarding the charity, and what your donation will be used for.
- ⇒ Never give social security numbers, bank account information, or credit/debit card information.
- ⇒ Pay by check made payable only to the charity. Never make cash donations.
- ⇒ Confirm the donation is tax deductible
- \Rightarrow Get a specific and detailed receipt.

Suspect Something?

Contact:

Better Business Bureau

By Telephone: 1-703-276-0100 Online: www.give.org

Florida Department of Agriculture and Consumer Services

By Telephone: 1-800-435-7352 Online: www.800helpfla.com

Internal Revenue Service

By Telephone: 1-877-829-5500 Online: www.irs.gov/charities



WISER/SIFMA

Just the Facts: Identity Theft and Credit Card Fraud



Introduction

M SCOTT

Senior financial abuse scams are a multi-billion dollar "industry." Studies estimate the annual financial loss nationwide to be around \$2.9 billion¹. In a recent New York State study, estimated annual losses for seniors in a subsample of New York State districts fell between \$352 million to \$1.5 billion, suggesting the national total may be substantially higher than previously estimated.² Although it can be difficult to measure the exact extent of the total financial loss, we know that these crimes are on the rise and continue to deprive seniors of their savings and

assets. These figures do not account for the tens of billions spent on indirect costs for medical care, social services, and legal costs, or for the pain and suffering of the victims. Victims are not only older people, but also their families and all who provide services and financial assistance.

All seniors, regardless of income, are at risk. Financial abuse may be perpetrated by anyone—a professional con artist, a paid caregiver, a stranger or casual acquaintance, or even a son, daughter, or other family member.

The following factors contribute to the prevalence of senior financial abuse:

- A high percentage of seniors live alone and may be more vulnerable to scams.
- Seniors may be trusting and readily believe the sales "pitches" they hear.
- The population of seniors is increasing, providing a continuous source of wealth for financial abusers.

WHAT IS IDENTITY THEFT?

Identity theft is the use of another person's personal information to commit theft or fraud.

WHAT IS CREDIT CARD FRAUD?

Credit card fraud is the unauthorized use of a credit/debit card to obtain money or property.

Education and awareness are two key strategies to preventing and responding to elder financial abuse. This brief describes two common types of abuse, identity theft and credit card fraud, and provides resources to keep seniors from becoming victims.

Identity Theft and Credit Card Fraud

Identity theft and credit card fraud are common types of senior financial abuse. In 2014, the Federal Trade Commission reported that 39% of the identity theft complaints, and nearly half (49%) of fraud complaints were from those 50 years of age and older.³



Identity theft crimes may happen without the senior's knowledge. Sometimes, the threat of physical violence or intimidation is also used to acquire the senior's personal information.

In cases of identity theft, perpetrators may obtain a senior's Social Security number, birth date, home address or other personal information and use it to redirect funds from banking accounts, take out loans in the senior's name, or open up new accounts. Often the perpetrators use phone and email scams to ask for personal information or obtain money from a senior in exchange for a prize or other promise of future services or financial reward.

How to Recognize Indicators of Identity Theft and Credit Card Fraud

- Changes in a senior's lifestyle—empty refrigerator, unexplained worries about finances
- Changes in an account's beneficiaries or authorized signers on debit/credit card accounts
- Denial of credit for no apparent reason
- Credit reports with information about accounts the senior did not open
- Unexplained debit or credit card charges or bills from unknown sources
- © Calls from companies, creditors or collection agencies about services or purchases the senior did not initiate
- IRS notice that more than one tax return was filed in the senior's name
- IRS notice about reported income from an employer the senior never worked for

How You Can Help Stop Identity Theft and Credit Card Fraud

Easy Steps To Protect Property and Assets

- Do not respond to personal sales pitches, phone calls, texts or e-mails that ask for personal information.
- Tell a caller or person at the door that you intend to call the authorities. Say "no" or just hang up.
- Don't use the same password for everything.
- Shred all documents with valuable and personal information, such as medical or financial records.
- Obtain credit reports! Everyone has a right to a free credit report every year from each of the three nationwide credit reporting companies. Order all three at once, or one every four months.
- 1 The MetLife Mature Market Institute. The MetLife Study of Elder Financial Abuse. June 2011.
- 2 New York State Office of Children and Family Service. The New York State Cost of Financial Exploitation Study June 15, 2016
- 3 Federal Trade Commission. 2014 Consumer Sentinel Network Data Book for January December 2014. February 2015.

To order, go to annualcreditreport.com or call 1-877-322-8228. This is the only source approved by the federal government to get a free credit report.

Register your phone numbers on the National Do Not Call Registry by calling 1-888-382-1222 or by going to www.donotcall.gov. Most legitimate sales people honor the Do Not Call list. Scammers don't, so be skeptical of random calls.

THE THREE NATIONWIDE CREDIT REPORTING COMPANIES

Equifax: www.equifax.com Experian: www.experian.com TransUnion: www.transunion.com

What To Do If You Believe Identity Theft or Credit Card Fraud Has Occurred

Immediately inform the credit card companies of suspected fraud and provide information on unauthorized purchases. Contact a nationwide credit reporting company (see box above) to obtain a credit report and check for irregularities.

Create an Identity Theft Affidavit through the Federal Trade Commission at www.identitytheft.gov or call 877-438-4338. This helps get fraudulent information removed from the credit reports and helps the authorities investigate the crime.

Take the Identity Theft Affidavit to the police and file a police report. These two documents, the affidavit and police report, constitute an Identity Theft report.

ADDITIONAL HELPFUL RESOURCES

Many public agencies are involved in preventing and detecting senior abuse and in prosecuting those who commit it. Many organizations are also dedicated to educating seniors on these topics:

- * FBI www.fbi.gov/scams-safety/fraud/seniors
 Provides information on fraud schemes and how to avoid them.
- Internet Crimes Complaint Center (IC3)
 The IC3 works with the FBI and other agencies to receive and refer internet crime complaints.
- National Center for Victims of Crime— www.victimsofcrime.org
 Financial Crime Resource Center

Helps victims of financial crime recover their assets and recover control of their lives.

- * Identity Theft Resource Center www.idtheftcenter.org

 Non-profit that provides victim and consumer support as well as public education.
- * Financial Fraud Enforcement Task Force www.stopfraud.gov Investigates suspected financial fraud.
- Postal Inspection Service www.postalinspectors.uspis.gov Investigates domestic and international fraud which uses the U.S. Mail.
- The Securities and Exchange Commission (SEC)
 Investigates securities fraud.
 1-800-732-0330
- * Consumer Financial Protection Bureau www.consumerfinance.gov/older-americans Provides resources to help protect seniors' financial assets.
- U.S. Administration on Aging
 In partnership with the National Association of Area Agencies on Aging,
 operates the Eldercare Locator to help individuals find local caregiving services and resources.

ADMINISTRATION ON AGING RESOURCE CENTERS

partner to provide valuable information to seniors, caregivers, families and communities across the nation.

National Resource Center on Women and Retirement Planning

National Resource Center on Women Retirement Planning The Women's Institute for a Secure Retirement (WISER), in partnership with the Administration on Aging, operates the National Resource Center on Women and Retirement Planning to provide user-friendly financial education and retirement planning tools for low-income women, women of color, and women with limited English speaking proficiency. WISER's mission is to inform women about the issues that affect their long-term financial security and to stress the

importance of taking an active role in planning for retirement. The Center specially tailors educational financial tools and information to meet the needs of the target population. Through the Center's one stop gateway, women have access to comprehensive, easily understood information that allows them opportunities to plan

for income during retirement and to plan for long-term care as they need it.

1140 19th Street, NW, Suite 550 Washington, DC 20036 (202) 393-5452 www.wiserwomen.org



New York

120 Broadway, 35th Floor New York, N.Y. 10271 212.313.1200

Washington, D.C.

1101 New York Avenue, NW 8th Floor Washington, D.C. 20005 202.962.7300

www.sifma.org



The Securities Industry and Financial Markets Association (SIFMA)

The Securities Industry and Financial Markets Association (SIFMA) is the voice of the nation's securities industry, bringing together the shared interests of hundreds of broker-dealers, banks and asset managers. SIFMA advocates for effective and resilient capital markets. WISER and SIFMA are proud to partner together to raise awareness about the problem of elder financial fraud and abuse, as well as provide education and resources to help prevent these crimes from occurring.

© Women's Institute for a Secure Retirement/SIFMA, 2016



Identity Theft

Here's how it works:

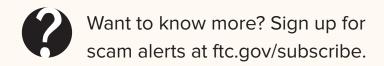
Someone gets your personal information and runs up bills in your name. They might use your Social Security or Medicare number, your credit card, or your medical insurance – along with your good name.

How would you know? You could get bills for things you didn't buy or services you didn't get. Your bank account might have withdrawals you didn't make. You might not get bills you expect. Or, you could check your credit report and find accounts you never knew about.

Here's what you can do:

- 1. Protect your information. Put yourself in another person's shoes. Where would they find your credit card or Social Security number? Protect your personal information by shredding documents before you throw them out, by giving your Social Security number only when you must, and by using strong passwords online.
- 2. Read your monthly statements and check your credit. When you get your account statements and explanations of benefits, read them for accuracy. You should recognize what's there. Once a year, get your credit report for free from AnnualCreditReport.com or 1-877-322-8228. The law entitles you to one free report each year from each credit reporting company. If you see something you don't recognize, you will be able to deal with it.







Please Report Identity Theft

If you suspect identity theft, act quickly. Please report it to the Federal Trade Commission.

- Call the FTC at 1-877-FTC-HELP (1-877-382-4357) or TTY 1-866-653-4261
- Go online: ftc.gov/complaint

The FTC operator will give you the next steps to take. Visit ftc.gov/idtheft to learn more.









40

Last year 10 million Americans suffered financial loss, personal embarrassment and frustration because someone - often a stranger they have never met, in another city, state or even another country - stole and misused their confidential financial information. You don't have to be wealthy or well-known to be a target. Victims include senior citizens, working people, teenagers, and even infants. Anyone with a Social Security number, bank account, or credit card is at risk.

CREDIT BUREAUS

To order your report, call: 800-685-1111 To report fraud, call: 800-525-6285

Experian

www.experian.com

To order your credit report or report fraud, call: 888-EXPERIAN (397-3742)

TransUnion

www.transunion.com

To order your report, call: 800-888-4213 To report fraud, call: 800-680-7289 or write: Fraud Victim Assistance Dept., P.O. Box 6790, Fullerton, CA 92834-6790

LEARN MORE ABOUT ID THEFT

Federal Trade Commission www.ftc.gov

New Mexico State Police www.dps.nm.org

Identity Theft Resource Center www.idtheftcenter.org

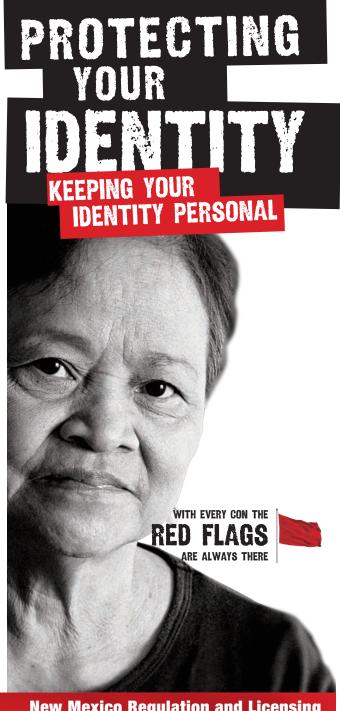


New Mexico Regulation and Licensing

Securities Division

2550 Cerrillos Rd Santa Fe, NM, 87505

1.800.704.5533 www.redflagsnm.com



New Mexico Regulation and Licensing Securities Division

redflagsnm.com | 1.800.704.5533

WHAT IS IDENTITY THEFT?

Identity theft is one of the fastest-growing crimes both in the U.S. and around the world. This form of fraud cost American businesses and consumers an estimated \$400 million last year alone. The average victim spends about \$1,400 in expenses and 600 hours in time to clear his or her name after personal financial information is stolen and misused.

The identity thief may loot your bank account, run up huge bills on your credit cards, obtain new credit cards in your name, and use your credit history to buy a car or borrow money from a bank. Using your Social Security number, a thief can even obtain a driver's license or passport in your name and use those documents to commit other crimes that you could be blamed for. Identity Theft victims can spend months or even years in untangling the confusion, restoring their credit rating, and clearing their names.

Banks, credit card issuers and law enforcement agencies are all taking steps to crack down on the crime of Identity Theft. But the first and most effective line of defense is with you.

GUARD YOUR PRIVACY

CLEAN OUT YOUR WALLET AND PURSE

Don't carry PIN numbers, checking account statements, Social Security card, or other confidential information with you.

SECURE PERSONAL INFORMATION AT HOME

Keep bank statements, credit card bills, tax returns and other financial records locked up where a thief is unlikely to find them.

GUARD YOUR MAIL AND SHRED YOUR TRASH

Keep track of your monthly bank and credit card statements to make sure you receive them. Foil "dumpster divers" by shredding or burning financial info before discarding it.

DON'T GIVE OUT CONFIDENTIAL INFORMATION OVER THE PHONE

No bank, mortgage lender, or government agency will call and ask you for your Social Security number, bank account number, PIN, or other private financial information. Be suspicious of anyone who does.

BE A WARY WEB SURFER

If you use your home computer to access the Internet, install "anti-virus" and anti-spyware software and update it regularly. Don't store confidential financial information on your computer hard drive.

ORDER A COPY OF YOUR CREDIT REPORT

At least once a year order a copy of your report from each of the three major credit rating agencies and review it carefully.

HOW THIEVES CAN STEAL YOUR PRIVATE INFORMATION

- They steal your wallet or purse containing your driver's license, credit and ATM cards, and other personal identification.
- They trick you into revealing information over the phone by impersonating government agents, law enforcement officers, bankers or mortgage lenders.
- They pilfer your mail, including bank and credit card statements, pre-approved credit card offers, new checks and tax returns.
- They file a bogus "change of address form" with the Post Office to divert your mail to another location.
- They rummage through your trash or trash discarded by restaurants, stores and other businesses - in search of personal data.
- They pose as a landlord, employer or someone else with a legitimate need for the information to obtain your confidential credit report.
- They burglarize your home to steal cancelled checks, tax returns, credit card bills, and other personal files.

- They scam you over the Internet by using e-mail to lure you to a legitimate-looking but fake web page that pretends to be a bank, mortgage lender, or government agency site.
- They steal files out of offices where you're a customer, employee, client or patient, sometimes by bribing an employee, or by "hacking" into the company's computers.
- They secretly plant "spyware" and other hidden software on your home computer to copy files, track your Internet use, or capture PIN numbers and passwords stored on your computer.

HOW TO FIGHT BACK

CONTACT THE CREDIT BUREAUS LISTED ON BACK

Report that another person is fraudulently obtaining credit in your name. Ask them to flag your file with a fraud alert and provide you with a copy of your current credit report. Review that report carefully and write to the credit bureaus asking them to remove items generated by the fraud.

CLOSE ANY BANK AND CREDIT ACCOUNTS THAT HAVE BEEN TAMPERED WITH

Do not cancel all your credit cards - it can be difficult to get new credit while you are clearing up the confusion.

CALL THE FTC'S IDENTITY THEFT HOTLINE TOLL-FREE AT 877-IDTHEFT 877-438-4338

Counselors will take your complaint and advise you on how to deal with the credit-related problems that could result. The FTC "ID Theft Affidavit" simplifies the process of disputing charges with companies where a new account was opened in your name but without your permission or knowledge.

FILE A COMPLAINT

Contact your local police or the police in the community where the identity theft took place. Keep a copy of that report.

WISER/SIFMA Just the Facts: HEALTHCARE SCAMS



Introduction

Senior financial abuse scams are a multi-billion dollar "industry." Studies estimate the annual financial loss nationwide to be around \$2.9 billion¹. In a recent New York State study, estimated annual losses for seniors in a subsample of New York State districts fell between \$352 million to \$1.5 billion, suggesting the national total may be substantially higher than previously estimated.² Although it can be difficult to measure the exact extent of the total financial loss, we know that these crimes are on the rise and continue to deprive seniors of their savings and assets. These figures do not account for the tens of billions spent on indirect costs for medical care, social services, and legal costs, or for the pain and suffering of the victims. Victims are not only older people, but also their families and all who provide services and financial assistance.

All seniors, regardless of income, are at risk. Financial abuse may be perpetrated by anyone—a professional con artist, a paid caregiver, a stranger or casual acquaintance, or even a son, daughter, or other family member.

The following factors contribute to the prevalence of senior financial abuse:

- A high percentage of seniors live alone and may be more vulnerable to scams.
- Seniors may be trusting and readily believe the sales "pitches" they hear.
- The population of seniors is increasing, providing a continuous source of wealth for financial abusers.

Education and awareness are two key strategies to preventing and responding to elder financial abuse. This brief describes common healthcare scams, and provides resources to keep seniors from becoming victims.

HEALTHCARE FRAUD COSTS THE COUNTRY **TENS OF BILLIONS OF DOLLARS A YEAR.**

-Source: FBI

Educate Yourself and Others About These Healthcare Scams

Medicare Fraud

Since every U.S. citizen or permanent resident is eligible for Medicare at age 65, seniors are a prime target for Medicare fraud. These scams trick seniors into providing their Medicare or Social Security number, and include:

- The promise of free services or groceries
- Phony "health surveys"
- Submitting fraudulent bills for services or medical equipment and identity theft

Open enrollment season for Medicare is a time of increased scams, as Medicare beneficiaries can make changes to their health plan and prescription coverage.

Scammers will pose as employees from the Centers for Medicare & Medicaid Services (CMS) or other government agencies, claiming that new cards are being issued. Do not respond to these requests; *the government will never solicit information over the phone or through email.* Learn more at www.stopmedicarefraud.gov.

Health Insurance and Marketplace Scams

Scammers have taken advantage of changes in the Affordable Care Act —to falsely present themselves as government officials or healthcare providers looking to "verify" personal information, such as Medicare ID numbers, bank account numbers, or credit cards. Also, email "phishing" scams are being targeted at Marketplace.gov consumers. The phishing emails claim to come from a U.S. Federal Government Agency. Any effort to solicit information from you for your health care should be regarded as suspicious. *Don't respond to emails and hang up on the callers*.



Counterfeit Prescription Drugs

Seniors often use the internet to look for better prices on



prescription drugs. Scammers will offer "special low prices" on fraudulent drugs. Reputable online pharmacies will have the Verified Internet Pharmacy Practice Site (VIPPS) seal of approval—look for it. Scammers secure credit card numbers and may continue to charge

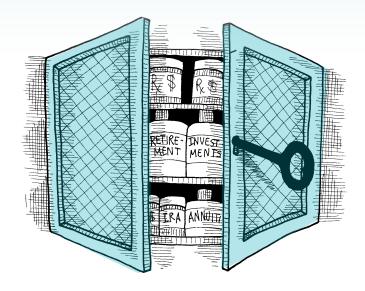
¹ The MetLife Mature Market Institute. The MetLife Study of Elder Financial Abuse. June 2011.

New York State Office of Children and Family Service. The New York State Cost of Financial Exploitation Study June 15, 2016

and bill seniors for subsequent "purchases" they did not initiate. Many seniors are unaware of what they are being billed for and will continue to pay the charges.

Medical Discount Cards

Discount cards are a low-cost way to get needed medical care. Consumers typically pay a monthly fee and gain access to a large pool of primary physicians, eye doctors, pediatricians and other providers at a discounted price. Many discount medical cards are fraudulent. They provide fake lists of providers, phony discounts, and high fees that are not readily apparent and often mimic health insurance but provide no actual benefits. Learn more about spotting a phony card at www.insurancefraud.org, under scam alerts.



Funeral and Cemetery Scams

Scammers may read obituaries and contact the grieving widow or widower claiming the deceased had an outstanding debt with them. Another tactic of disreputable funeral homes is to insist that a casket, one of the most expensive parts of funeral services, is necessary, even in the case of cremation.

ADDITIONAL HELPFUL RESOURCES -

Many public agencies are involved in preventing and detecting senior abuse and in prosecuting those who commit it. Many organizations are also dedicated to educating seniors on these topics:

Medicare

www.stopmedicarefraud.gov or 1-800-MEDICARE

The U.S. Department of Health and Human Services publishes a helpful booklet called *Protecting Yourself* and Medicare from Fraud. Also, the Senior Medicare Patrol helps with detecting and preventing healthcare fraud and abuse.

Senior Medicare Patrol

www.smpresource.org

Find trained volunteers in your area who can help Medicare beneficiaries and their families prevent, detect and report healthcare fraud, errors and abuse.

FBI www.fbi.gov/scams-safety/fraud/seniors Provides information on fraud schemes and how to avoid them.

www.ftc.gov Protects consumers from unfair, deceptive, and fraudulent business practices.

National Center on Elder Abuse

www.ncea.acl.gov

Provides state resources: helplines, hotlines and information.

U.S. Administration on Aging

www.eldercare.gov 1-800-677-1116

In partnership with the National Association of Area Agencies on Aging, operates the Eldercare Locator to help individuals find local caregiving services and resources.

ADMINISTRATION ON AGING RESOURCE CENTERS

partner to provide valuable information to seniors, caregivers, families and communities across the nation.

National Resource Center on Women and Retirement Planning

National Resource Center on Women Retirement Planning The Women's Institute for a Secure Retirement (WISER), in partnership with the Administration on Aging, operates the National Resource Center on Women and Retirement Planning to provide user-friendly financial education and retirement planning tools for low-income women, women of color, and women with limited English speaking proficiency. WISER's mission is to inform women about the issues that affect their long-term financial security and to stress the

importance of taking an active role in planning for retirement. The Center specially tailors educational financial tools and information to meet the needs of the target population. Through the Center's one stop gateway, women have access to comprehensive, easily understood information that allows them opportunities to plan

for income during retirement and to plan for long-term care as they need it.

1140 19th Street, NW, Suite 550 Washington, DC 20036 (202) 393-5452 www.wiserwomen.org



New York

120 Broadway, 35th Floor New York, N.Y. 10271 212.313.1200

Washington, D.C.

1101 New York Avenue, NW 8th Floor Washington, D.C. 20005 202.962.7300

www.sifma.org



The Securities Industry and Financial Markets Association (SIFMA)

The Securities Industry and Financial Markets Association (SIFMA) is the voice of the nation's securities industry, bringing together the shared interests of hundreds of broker-dealers, banks and asset managers. SIFMA advocates for effective and resilient capital markets. WISER and SIFMA are proud to partner together to raise awareness about the problem of elder financial fraud and abuse, as well as provide education and resources to help prevent these crimes from occurring.

© Women's Institute for a Secure Retirement/SIFMA, 2016 -



Health Care Scams

Here's how they work:

You see an ad on TV, telling you about a new law that requires you to get a new health care card. Maybe you get a call offering you big discounts on health insurance. Or maybe someone says they're from the government, and she needs your Medicare number to issue you a new card.

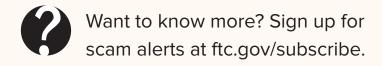
Scammers follow the headlines. When it's Medicare open season, or when health care is in the news, they go to work with a new script. Their goal? To get your Social Security number, financial information, or insurance number.

So take a minute to think before you talk: Do you really have to get a new health care card? Is that discounted insurance a good deal? Is that "government official" really from the government? The answer to all three is almost always: No.

Here's what you can do:

- 1. Stop. Check it out. Before you share your information, call Medicare (1-800-MEDICARE), do some research, and check with someone you trust. What's the real story?
- Pass this information on to a friend. You probably saw through the requests. But chances are you know someone who could use a friendly reminder.







Please Report Scams

If you spot a health care scam, please report it to the Federal Trade Commission.

- Call the FTC at 1-877-FTC-HELP (1-877-382-4357) or TTY 1-866-653-4261
- Go online: ftc.gov/complaint

Your complaint can help protect other people. By filing a complaint, you can help the FTC's investigators identify scam artists and stop them before they can access to a friend's hard-earned money. It really makes a difference.









48

Elder Consumer Protection Program

The Elder Consumer Protection Program at Stetson University College of Law's Center for Excellence in Elder Law is an educational and information resource on general and legal matters regarding elder consumer protection and awareness. The program, which is supported by state funding, offers assorted materials and various services that provide and promote general knowledge, public awareness and assistance, and professional development and training.

The information contained herein is intended only as a brief overview on matters of general interest. It is not offered as legal advice, is not a definite statement of law, and is not a complete analysis of the area of law.

The applicability of law to a particular matter requires an exhaustive examination of the specific facts with the appropriate laws. If you have a specific legal issue or legal concern, you should always consult with an attorney for detailed legal advice.





ELDER CONSUMER PROTECTION PROGRAM

CENTER FOR EXCELLENCE IN **ELDER LAW**

> 1401 61st Street South Gulfport, Florida 33707

Phone: (727) 562-7888 Fax: (727) 345-1838

Email: ecpp@law.stetson.edu

Web: www.stetson.edu/law/elderconsumers

Twitter: @StetsonLawECPP

Identity Theft Awareness

Are YOU At Risk?

What is it?

How does it occur?

What can you do?



STETSONLAW

STETSON UNIVERSIT

Center for Excellence in Elder Law ACCESS AND JUSTICE FOR ALL®

© 2015 Stetson University College of Law. All Rights Reserved.

49



ACCESS AND JUSTICE FOR ALL®

What is Identity Theft?

According to the Federal Trade Commission (FTC), identity theft occurs when someone, without your permission, uses your personally identifying information to commit fraud or other crimes.

Personally Identifying Information Includes:

- Name
- Date of Birth
- Social Security Number
- Credit and Debit Card Numbers and PINs
- Bank and Financial Account Information
- Military ID Information
- Medical Insurance Information
- Pension Benefits Information



How Does Identity Theft Occur?

- Old Fashioned Stealing: Taking your wallet, purse or other belongings to obtain personal information.
- <u>Mail Theft</u>: Taking your incoming or outgoing mail from your mailbox to obtain personal information.
- **<u>Dumpster Diving</u>**: Rummaging through the trash for personal information.
- **Skimming:** Copying your credit/debit card numbers with special electronic storage devices when you use your card.
- <u>Phishing</u>: Pretending to be businesses, companies or financial institutions to obtain personal information in person, by telephone, by e-mail or on the Internet.
- **Shoulder-surfing:** Looking and listening for personal information, such as ATM pin numbers, credit/debit card numbers, or financial account numbers, while you are in public, on the telephone, or at a computer.

Suspect Something?
File a fraud report with the FTC
By telephone: 1-877-382-4357
Online: www.ftccomplaintassistant.gov

Help Protect Yourself

Credit Report: Allows consumers to review and monitor their credit file for unfamiliar activity.

Consumers may receive a free credit report from each of the three major credit reporting bureaus every twelve months.



By telephone: 1-877-322-8228

Online: www.annualcreditreport.com

Fraud Alert: Informs creditors to contact the consumer by telephone to verify that the consumer really wants to open a new account or get new credit. It is effective for 90 days but may be reactivated. Upon activation with one, the fraud alert is effective with all three major credit reporting bureaus:

Equifax: 1-888-766-0008 Experian: 1-888-397-3742 TransUnion: 1-800-680-7289

Credit Freeze: Prevents access to a consumer's credit file, limiting anyone trying to open up a new account or get new credit. It does not affect your credit score and can be temporarily lifted to allow access. Credit freeze laws vary by state. For additional information, visit www.consumersunion.org/research/security-freeze/

WISER/SIFMA

Just the Facts: Senior Financial Fraud and Abuse



Introduction

Senior financial abuse scams are a multi-billion dollar "industry." Studies estimate the annual financial loss nationwide to be around \$2.9 billion¹. In a recent New York State study, estimated annual losses for seniors in a subsample of New York State districts fell between \$352 million to \$1.5 billion, suggesting the national total may be substantially higher than previously estimated.² Although it can be difficult to measure the exact extent of the total financial loss, we know that these crimes are on the rise and continue to deprive seniors of their savings and assets. These figures do not account for the tens of billions spent on indirect costs for medical care, social services, and legal costs, or for the pain and suffering of the victims. Victims are not only older people, but also their families and all who provide services and financial assistance.

All seniors, regardless of income, are at risk. Financial abuse may be perpetrated by anyone—a professional con artist, a paid caregiver, a stranger or casual acquaintance, or even a son, daughter, or other family member.

The following factors contribute to the prevalence of senior financial abuse:

- A high percentage of seniors live alone and may be more vulnerable to scams.
- Seniors may be trusting and readily believe the sales "pitches" they hear.
- The population of seniors is increasing, providing a continuous source of wealth for financial abusers.

and abuse victimizes
hundreds of thousands of
seniors each year. Older
Americans hold the largest
percentage of the nation's
wealth, making them
prime targets for scammers, con artists and other
unethical professionals and
even family members.

Education and awareness are two key strategies to preventing and responding to elder financial abuse. This brief describes some common types of financial fraud and abuse and provides resources to keep seniors from becoming victims.

Types of Senior Financial Abuse

There are many different ways seniors are scammed and defrauded:

- Fraud: Using a senior's vulnerability to convince the senior to hand over property, money or valuable information under false pretenses.
- **Theft:** The wrongdoer takes property or assets directly from the senior.

Scammers and con artists are always coming up with new ways to rob seniors of their money and other assets. Educate yourself and others about common scams and swindles, and stay current on the latest scams by visiting www.fbi.gov/scams-safety/fraud/seniors

Common types of Senior Financial Abuse include:

WHO ARE THE VICTIMS?

- Most are between the ages of 80 and 89
- Women are twice as likely as men to be victimized
- Most live alone
- Most require some level of help with either health care or home maintenance

WHO ARE THE PERPETRATORS?⁴

- Strangers: 51%
- Family/Friends/Neighbors: 34%
- Business: 12%
- Medicare/Medicaid Providers: 4%
- 60% of known perpetrators are men, mostly between the ages of 30 and 59
- Women perpetrators tend to be younger, mostly between the ages of 30 and 49

Telemarketing and Internet Fraud

Targeting victims through the mail, phone, or email—characterized by aggressive tactics along with the use of false promises of cash prizes, goods, or services in exchange for paying fees or making purchases.

Identity Theft and Credit Card Fraud

Gaining access to a senior's personal information to take money and property. Includes tax ID theft where a scammer uses a senior's Social Security number to file a tax return and steal the refund, or impersonates the IRS and tells the senior that the IRS is owed money. If you suspect fraud, go to http://oig.ssa.gov/report-fraud-waste-or-abuse.

Grandparent Scam

Pretending to be a grandchild in trouble in order to convince the senior to wire money or send prepaid debit cards.

Sweepstakes and Lottery Scams

A widely practiced form of telemarketing fraud, scammers tell seniors that they have won a lottery or sweepstakes. The catch is, the senior must make a small payment or pay a fee to receive the alleged prize. Seniors may also receive a fake check back from the scammer, which will "bounce" after it gets deposited.

Investment Schemes & Fraud

Unscrupulous professional investors try to sell inappropriate, unethical, or confusing investment products to seniors, or from con artists claiming to be the "Nigerian prince" or some other wealthy foreigner who asks for your bank account number to transfer millions of dollars into your banking account.

Healthcare Scams

Getting information about a senior's medical accounts —like Medicare and Medicaid—in order to make fraudulent claims and take advantage of these taxpayer programs.

- 1 The MetLife Mature Market Institute. The MetLife Study of Elder Financial Abuse. June 2011.
- 2 New York State Office of Children and Family Service. The New York State Cost of Financial Exploitation Study June 15, 2016
- 3 The MetLife Mature Market Institute, op.cit.
- 4 Ibid.

How Can I Help Stop Elder Financial Abuse?

Educate seniors and their caregivers about financial abuse risks and what to look for. Pay attention to possible signs of financial abuse among your family members, friends and clients. Stay knowledgeable about your community's resources so you can provide caregivers with current up—to—date information. If there are signs of wrongdoing, contact Adult Protection Services and file a report with the local police department.

What is the Role of Adult Protective Services (APS)?

APS programs are state and local agencies authorized under state law to investigate reports of abuse, neglect and financial exploitation of older persons and adults with disabilities. APS interventions include:

- Receiving and investigating reports of senior abuse
- Developing a case plan and interventions, based on the victim's wishes
- Arranging for emergency housing, medical care, legal assistance, etc.
- Coordinating with other agencies to address abuse as comprehensively as possible



ADDITIONAL HELPFUL RESOURCES

Many public agencies are involved in preventing and detecting senior abuse and in prosecuting those who commit it. Many organizations are also dedicated to educating seniors on these topics:

National Center on Elder Abuse State Resources: Helplines, Hotlines and Information. www.ncea.acl.gov

* FBI www.fbi.gov
Provides information on fraud schemes and how to avoid them.

National Center for Victims of Crime

Financial Crime Resource Center

www.victimsofcrime.org

Helps victims of financial crime recover their assets and recover control of their lives.

* Consumer Financial Protection Bureau www.consumerfinance.gov Ensures that consumers get the information they need to make sound financial decisions.

Federal Trade Commission www.ftc.gov
Protects consumers from unfair, deceptive and fraudulent business practices.

* Financial Fraud Enforcement Task Force www.stopfraud.gov Investigates suspected financial fraud.

* Postal Inspection Service www.postalinspectors.uspis.gov Investigates domestic and international fraud which uses the U.S. Mail.

The Securities and Exchange Commission (SEC) www.investor.gov Investigates securities and investment fraud.
1-800-732-0330

U.S. Administration on Aging
 In partnership with the National Association of Area Agencies on Aging,
 operates the Eldercare Locator to help individuals find local caregiving services and resources.

ADMINISTRATION ON AGING RESOURCE CENTERS

partner to provide valuable information to seniors, caregivers, families and communities across the nation.

National Resource Center on Women and Retirement Planning

National Resource Center on Women Retirement Planning The Women's Institute for a Secure Retirement (WISER), in partnership with the Administration on Aging, operates the National Resource Center on Women and Retirement Planning to provide user-friendly financial education and retirement planning tools for low-income women, women of color, and women with limited English speaking proficiency. WISER's mission is to inform women about the issues that affect their long-term financial security and to stress the

importance of taking an active role in planning for retirement. The Center specially tailors educational financial tools and information to meet the needs of the target population. Through the Center's one stop gateway, women have access to comprehensive, easily understood information that allows them opportunities to plan

for income during retirement and to plan for long-term care as they need it.

1140 19th Street, NW, Suite 550 Washington, DC 20036 (202) 393-5452

www.wiserwomen.org



New York

120 Broadway, 35th Floor New York, N.Y. 10271 212.313.1200

Washington, D.C.

1101 New York Avenue, NW 8th Floor Washington, D.C. 20005 202.962.7300

www.sifma.org



The Securities Industry and Financial Markets Association (SIFMA)

The Securities Industry and Financial Markets Association (SIFMA) is the voice of the nation's securities industry, bringing together the shared interests of hundreds of broker-dealers, banks and asset managers. SIFMA advocates for effective and resilient capital markets. WISER and SIFMA are proud to partner together to raise awareness about the problem of elder financial fraud and abuse, as well as provide education and resources to help prevent these crimes from occurring.

© Women's Institute for a Secure Retirement/SIFMA, 2016 -

We all like to believe we're good judges of character, able to spot an honest man by the look in his eye, the tone of his voice, and the strength of his handshake. Appearances can be deceiving, financial predators are experts at deception. "Con" is short for "confidence," and a successful con artist relies on his ability to appear honest and trustworthy even as he cheats you of your money.

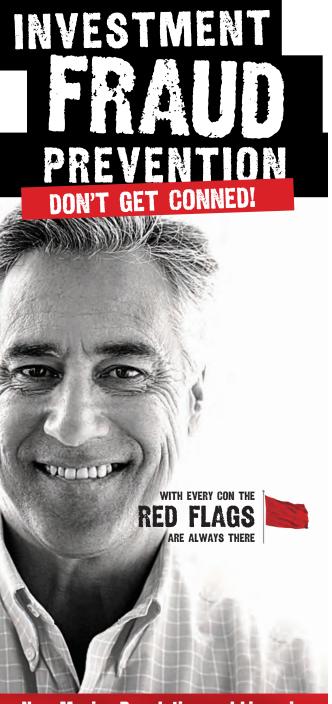


New Mexico Regulation and Licensing

Securities Division

2550 Cerrillos Rd Santa Fe, NM, 87505

1.800.704.5533 www.redflagsnm.com



New Mexico Regulation and Licensing Securities Division

redflagsnm.com | 1.800.704.5533

CHECK BEFORE YOU INVEST

CON ARTISTS ARE EXPERTS AT GAINING YOUR CONFIDENCE

No matter how good it sounds, treat any investment offer with extreme caution. Whether you hear about the opportunity through an e-mail or phone call, or from a friend or business contact, be certain to check out both the person and the investment he or she is promoting, before you write a check!

ASK QUESTIONS, THEN CHECK THE ANSWERS

Savvy investors take the time to do their own research. Don't rely on oral promises or representations. Get a full explanation of the proposed investment in writing, and make sure that you fully understand how this investment works and what the risks are.

CALL THE NEW MEXICO SECURITIES DIVISION

Confirm that the person you are dealing with is a licensed investment professional in New Mexico, and whether he or she has ever been disciplined or has any complaints pending.

BEFORE BUYING ANY STOCK, REVIEW FINANCIAL STATEMENTS

The company is required to file these with the Securities and Exchange Commission.

DON'T BE TALKED INTO TREATING ANY INVESTMENT OFFER AS "SECRET" OR "CONFIDENTIAL"

Have the documents reviewed by an attorney, tax adviser or someone you trust who understands investing.

INVESTMENT FRAUD COMES IN A VARIETY OF DISGUISES

PONZI SCHEMES

In a Ponzi, the con artist attracts investors by promising unrealistically high returns, and uses some of the money obtained from new victims to pay earlier participants some return. The scheme lasts only as long as the promoter can continue to lure in new victims.

PYRAMIDS

Often disguised as multi-level marketing opportunities or even charitable endeavors, pyramids require victims to go out and recruit a certain number of new participants in order to "rise up" the pyramid and collect their promised reward. In this way, pyramid schemes spread through families and communities, preying on the mutual trust people have in their friends, neighbors and co-workers.

PUMP AND DUMP STOCK SCAMS

In this fraud, unscrupulous promoters obtain large blocks of stock in a small, publicly traded company. With high-pressure telephone sales, mass e-mails and phony 'newsletters,' the promoters use false rumors about the company's prospects to drive up the stock price. When the promoters dump their shares at a profit, the other investors are left holding worthless stock.

LIMITED PARTNERSHIPS

These are investment vehicles in which investors purchase a share in a business venture such as drilling oil or gas wells, making a movie, or developing a real estate project. While partnerships may be genuine investments, con artists can defraud investors by misrepresenting the risks and potential profits, or by manipulating the enterprise to drain off the revenues in "expenses."

PROMISSORY NOTES

Promissory notes can be a legitimate tool for businesses that need to borrow money for short periods. It's not investment fraud as long as the borrower discloses all the risks, and provides you with the information you need to make an

informed decision. It is a fraud when backed by a nonexistent company, or promoted by promising high returns with little or no risk.

GLOBAL BANK SCHEMES

In these scams the promoter offers a 'risk free' opportunity to earn high returns by investing in exotic-sounding financial instruments traded in the global financial markets. The investment is often presented as a secret strategy shared only by very wealthy, sophisticated investors. In fact, the 'major world bank' may be no more than a fancy letterhead or a fake web page. Although the con artist may move the money overseas through foreign banks to cover his tracks, there is no real investment.

WARNING SIGNS

- The promoter claims to have secret, inside, or non-public information that he is willing to let you in on, but you need to keep it confidential. He is trying to get you to act without getting an outside opinion or checking his story with the authorities.
- with higher-than-market rate returns should ring alarm bells for you. There is no risk free investment. And the higher the return offered, the more risk you're taking with your money. Something is wrong when a promoter promises to make you eye-popping returns on your investment with little or no risk.
- "Act Now" or "Don't miss out on this once-in-a-lifetime opportunity." High pressure tactics intend to get you to make a snap decision without thinking it through. The promoter doesn't want you to take time to check his story.
- If it sounds to good to be true, it probably is. Compare promised yields with current returns on well-known stock indexes. Any investment opportunity that claims you'll get substantially more is certain to be highly risky.

Elder Consumer Protection Program

The Elder Consumer Protection Program at Stetson University College of Law's Center for Excellence in Elder Law is an educational and information resource on general and legal matters regarding elder consumer protection and awareness. The program, which is supported by state funding, offers assorted materials and various services that provide and promote general knowledge, public awareness and assistance, and professional development and training.

The information contained herein is intended only as a brief overview on matters of general interest. It is not offered as legal advice, is not a definite statement of law, and is not a complete analysis of the area of law.

The applicability of law to a particular matter requires an exhaustive examination of the specific facts with the appropriate laws. If you have a specific legal issue or legal concern, you should always consult with an attorney for detailed legal advice.





ELDER CONSUMER PROTECTION PROGRAM

CENTER FOR EXCELLENCE IN ELDER LAW

1401 61st Street South Gulfport, Florida 33707

Phone: (727) 562-7888 **Fax:** (727) 345-1838

E-mail: ecpp@law.stetson.edu

Web: www.stetson.edu/law/elderconsumers

Twitter: @StetsonLawECPP



STETSON UNIVERSITY

Center for Excellence in Elder Law

ACCESS AND JUSTICE FOR ALL®

© 2015 Stetson University College of Law. All Rights Reserved.

Current & Common Scams (2015)

Grandparent Scam

Lottery / Sweepstakes Scam

IRS Scam

Technical Assistance Scam

Work From Home Scams





Center for Excellence in Elder Law

ACCESS AND JUSTICE FOR ALL®

Relative in Need/Grandparent

Scam: Generally comes in two different varieties: The Scammer pretending to be your relative or a friend of your relative; or claiming to be the authorities. In both scenarios the Scammer will claim that your relative is in trouble and needs money wired to them to help.

IRS Scam: Scammer calls and claims to be from the Internal Revenue Service and states that you owe back taxes. The Scammer will threaten you with arrest and jail time if you do not comply, or will state that there is already a warrant out for your arrest.

Lotter / Sweepstakes Scam (Jamaican Lottery): Scammer will call and claim that you have won a prize. However, to claim the prize you must first pay taxes, insurance, shipping, etc.

Fraud Avoidance Measures

Sign up for the Do Not Call List

Screen ALL Unknown Phone Calls

NEVER Wire Money

Shred ALL Sensitive Documents

Use Direct Deposit

Never give out Personal Information unless YOU initiated the contact

Technical Assistance Scam: Scammer will call and claim to be from Windows, Microsoft, Norton Antivirus, etc. and will request that you access your computer. The Scammer will then instruct you to access a program that shows the number of systems errors in Windows. The Scammer will then claim that your computer is messed up and in need of repair. The Scammer's goal is for to gain remote access to your computer and steal your personal information.

Robo Calls / Payday Loan Scam: Scammer will call and state that you have been approved for a high level loan, and that to complete the process and receive their funds you need to visit a website and enter your personal information.



If you become a Target of a Scam, Contact:

Your Local Law Enforcement Agency

The Florida Attorney General: www.myfloridalegal.com or 1-866-NO-SCAM

The Federal Trade Commission: www.ftccomplaintassistant.gov or 1-877-FTC-HELP

Visit www.stopfraud.gov to determine which other Federal Agencies to report to.

Work from Home Scams: Come in a number of Varieties. Most Common Are:

Foreign Money Scam (Nigerian or 419 Scam): Offer to help transfer money into the US from a foreign country, earning a commission in the process.

"Busy Work" Scams: Includes Envelope Stuffing, Crafting, etc. Often, the Scammer will "overpay" you for your work, and will request that you send a check or wire the excess money back to them. The original "paycheck" is fake however, so any money you send them will be your own money.

Reshipping Scams: Offer to Receive and Reship various items from your home, earning a commission for each item shipped. Generally, the items are stolen.

Work from Home Scams are extremely dangerous. Not only can your time and money be stolen, but you can unwittingly become an Accomplice to Fraud and can be found criminally liable for Money Laundering, Receiving Stolen Property, Mail Fraud, and Wire Fraud.

Remember: If it sounds too good to be true, it is!

Elder Consumer Protection Program

The Elder Consumer Protection Program at Stetson University College of Law's Center for Excellence in Elder Law is an educational and information resource on general and legal matters regarding elder consumer protection and awareness. The program, which is supported by state funding, offers assorted materials and various services that provide and promote general knowledge, public awareness and assistance, and professional development and training.

The information contained herein is intended only as a brief overview on matters of general interest. It is not offered as legal advice, is not a definite statement of law, and is not a complete analysis of the area of law.

The applicability of law to a particular matter requires an exhaustive examination of the specific facts with the appropriate laws. If you have a specific legal issue or legal concern, you should always consult with an attorney for detailed legal advice.





ELDER CONSUMER PROTECTION PROGRAM

CENTER FOR EXCELLENCE IN ELDER LAW

1401 61st Street South Gulfport, Florida 33707

Phone: (727) 562-7888 **Fax:** (727) 345-1838

E-mail: ecpp@law.stetson.edu

Web: www.stetson.edu/law/elderconsumers

Twitter: @StetsonLawECPP



STETSON UNIVERSITY

Center for Excellence in Elder Law

ACCESS AND JUSTICE FOR ALL®

 $\ensuremath{\mathbb{G}}$ 2015 Stetson University College of Law. All Rights Reserved.

Top Scams Targeting Veterans

VA Phishing

Pension/Aid and Attendance

Veterans Benefits Buyout

Fake Charities

Affinity Fraud





Center for Excellence in Elder Law

ACCESS AND JUSTICE FOR ALL®

Why Scammers Target Veterans

Like members of the active duty military, many Veterans receive steady monthly paychecks through VA benefits or military retirement. Veterans are also typically a very motivated lot, watch out for one another, and give freely of both their time and money. Scammers know and attempt to exploit these facts in order to swindle many well meaning Veterans out of their hard earned money. This brochure is intended as a guide to help Veterans spot the most prevalent scams and swindles targeting the Veteran population.



Affinity Fraud: More of a method than a scam itself, Affinity Fraud occurs when the Scammer claims to be a Veteran or working for a Veteran's Organization in order to gain the trust and confidence of other Veterans.

Bogus Sales / The Deployment Scam:

Scammers will post on websites that offer classified ads claiming to be a service member who is being deployed and needs to sell an expensive item, such as a car or a flat screen television, in a hurry and at a discount. The scammer will ask for a wire transfer of the payment of upfront fees. This is a sure sign of a scam, NEVER wire money for any purchase.

VA Phishing Scam: The Scammer will call a Veteran stating that they work for the Department of Veterans Affairs and claiming that they need to update the Veteran's personal information. Be Aware, the VA will NEVER ask you for your sensitive personal information by phone, Email, or text.

Investment/Pension Scam: Scammers claiming to be "Veterans Financial Advocates" will claim that a Veteran is entitled to additional benefits. The Scammers often want to review the Veteran's investment portfolio, and will attempt to get the Veteran to invest in an irrevocable trust or annuity so that the Veteran appears to have fewer assets then they really have, entitling them to an additional pension as well as Aid and Attendance benefits. This DOES NOT WORK, and may actually cause the Veteran to lose some of their VA benefits, lose eligibility for Medicaid services, or will cut the Veteran off from their money for a significant amount of time.

Veterans Benefits Buyout Scam: Scammers target Veterans in need of quick cash, offering an upfront cash payment in exchange for their future disability or pension payments and benefits. However, these

buyouts are typically only 30-40% of what the value of the benefit actually is, and are structured in such a way that they are harmful to the Veteran's finances.

Charging for Military Records and Forms:

A well known Scam that is still very prevalent. Here, the Scammer tricks the Veteran into paying for information that is already available to the Veteran for free, such as military records and government forms.

Fake Charities: Fake charities will use names that closely resemble those of a legitimate charity; reference the Armed Forces, a particular branch of the military, or a specific military unit; or include the words "Veteran" or "Military Family" in order to make themselves seem legitimate. To determine if a charity is legitimate, visit the Better Business Bureau's Wise Giving Alliance at www.give.org and Charity Watch at www.charitywatch.org

Rental/Real Estate Scams: A Scammer will post a fake rental property or real estate listing on classified add websites promising military discounts and too-good-to-be-true incentives. Typically, the Scammer will use the address and pictures of a legitimate property to trick the Veteran into wiring a security deposit or down payment to the landlord. Veterans should NEVER wire money for any purchase or rental, as wiring money is the same as sending cash, which makes challenging the "purchase" and recovering the lost funds very difficult.

