MONEY SMART for Older Adults

Resource Guide

June 2021

cfpb Consumer Financial Protection Bureau

FDIC FEDERAL DEPOSIT INSURANCE CORPORATION

Welcome to Money Smart for Older Adults!

Financial exploitation has been called "the crime of the 21st century" with one study suggesting that older Americans lost at least $2.9 billion to financial exploitation in 2010[1] by a broad spectrum of perpetrators, including persons they know and trust, as well as strangers. Cognitive impairment diminishes the ability of some older adults to make financial decisions and to detect frauds and scams.

This epidemic is under the radar. The cases tend to be very complex and can be difficult to investigate and prosecute. Elders who lose their life savings usually have little or no opportunity to regain what they have lost. Elder financial exploitation can result in the loss of the ability to live independently. It can also result in a decline in health, broken trust, and fractured families.

Awareness is the first step. Planning ahead for financial wellbeing and the possibility of diminished financial capacity is critical. Reporting and early intervention are vital to preventing loss and recovering loss when possible.

Money Smart for Older Adults is designed to provide you with information and tips to help prevent common frauds, scams and other types of elder financial exploitation in your community. Please share this information with others.

[1] The MetLife Study of Elder Financial Abuse: Crimes of Occasion, Desperation, and Predation against America's Elders (New York, NY: MetLife, June 2011) [available at **https://vtechworks.lib.vt.edu/bitstream/handle/10919/24184/mmi_elder_financial_abuse_2011.pdf**].

Acknowledgements

The Federal Deposit Insurance Corporation (FDIC) and (CFPB) thank the following agencies for contributing to the information covered in this course:

- U.S. Department of Health and Human Services, Administration for Community Living–Senior Medicare Patrol
- Federal Trade Commission
- Securities and Exchange Commission
- Social Security Administration
- Financial Industry Regulatory Authority, Inc.[1]
- Internal Revenue Service

[1] The Financial Industry Regulatory Authority, Inc. (FINRA) is a non-governmental organization. The CFPB and FDIC are not affiliated with and do not endorse FINRA or any other private entity, product, or service referenced in this guide, nor do they make any representations or warranties about the capabilities or quality of the entities, products or services referenced. There may be other entities, products or services not referenced here that also may serve your needs. The CFPB and FDIC are not responsible for any losses or other problems you experience in connection with particular products or services you choose to use.

Table of Contents

Checking In

Welcome

Welcome to *Money Smart for Older Adults*! By taking this module, you'll learn important points to consider in planning for a more secure financial future, including how to guard against identity theft and other forms of financial exploitation, as well as how to prepare financially for unexpected life events and disasters.

Objectives

After completing this module, you will be better able to:

- Recognize and reduce the risk of elder financial exploitation
- Guard against identity theft
- Plan for possible loss of your ability to manage your finances
- Prepare financially for disasters
- Find other helpful resources for managing your money and reporting financial exploitation

Participant Materials

The Resource Guide contains:

- Information on how to identify and report financial exploitation
- Resources and information on protecting your assets
- Activities to help you learn the material
- Tools and instructions to complete the activities
- A glossary of the terms used in this module

Getting Started

Let's start by establishing an understanding of elder financial exploitation. Financial exploitation is a type of elder abuse. Elder abuse can take many forms, alone or in combination, including physical, psychological, emotional, or sexual abuse, neglect, abandonment, and self-neglect.

What is elder financial exploitation?

Financial exploitation is the fraudulent or otherwise illegal, unauthorized, or improper actions by a caregiver, fiduciary, or other individual in which the resources of an older person are used by another for personal profit or gain; or actions that result in depriving an older person of the benefits, resources, belongings, or assets to which they are entitled.

Elder financial exploitation is the theft of money, property or belongings.

Who is at risk for elder financial exploitation?

Anyone can be the victim of financial exploitation. Financial exploitation crosses all social, educational, and economic boundaries.

Why are older adults at risk of financial exploitation?

The following circumstances or conditions, especially in combination, can make an older adult more vulnerable to financial exploitation.

Some older adults may:

- Have regular income and accumulated assets.
- Be trusting and polite.
- Be lonely and socially isolated.
- Be vulnerable due to grief from the loss of a spouse, family member, friend, or pet.

- Be reluctant to report exploitation by a family member, caregiver, or someone they depend on.
- Be dependent on support from a family member or caregiver to remain independent.
- Be receiving care from a person with substance abuse, gambling or financial problems, or mental health issues.
- Fear retaliation by the exploiter.
- Be unfamiliar with managing financial matters.
- Not have planned for the potential loss of decision-making capacity.
- Be cognitively impaired with diminished ability to make financial decisions or detect a fraud or scam.
- Be dependent on a family member, caregiver or another person who may pressure them for money or control of their finances.

What are some examples of financial exploitation?

- Exploitation by an agent under a power of attorney or person in another type of fiduciary relationship (see glossary for definition of fiduciary)
- Theft of money or property, often by a family member, caregiver or in-home helper
- Investment fraud and scams, including deceptive "free-lunch seminars" selling unnecessary or fraudulent financial services or products
- Lottery and sweepstakes scams
- Grandparent/imposter scams
- Tax and debt collection scams
- Charity scams

- Scams by telemarketers, mail offers or door-to-door salespersons
- Computer and Internet scams
- Identity theft
- Reverse mortgage fraud
- Contractor fraud and home improvement scams

Who are the abusers?

Perpetrators of financial exploitation can be:

- Family members and caregivers
- Friends, neighbors or acquaintances
- Agents under a power of attorney or others with legal authority to manage your money or property
- Romance scams
- Telephone and mail scammers
- Fraudulent debt collectors
- Financial advisers
- Internet scammers
- Home repair contractors
- Medicare scam operators
- Other persons known or unknown to the older adult

Why don't older adults report financial exploitation?

- **Shame and embarrassment** – Many people are ashamed to admit that they have been financially exploited.
- **Loyalty** – Older adults may be reluctant to report a family member, caregiver or other person who may treat them well in other ways.
- **Fear of retaliation** – Older adults might fear not being believed or losing their independence by being declared incompetent and moved into a "nursing home."
- **Dependence** – Victims may be dependent on the abuser for care or assistance.
- **Denial** – Some victims are unwilling or unable to acknowledge that financial exploitation is happening to them.
- **Self-blame** – Abuse can erode an older person's self-esteem, and some victims may believe they deserve or have caused the abuse.
- **Lack of awareness** – Some victims are unaware that they are being exploited, or don't know to whom they can report financial exploitation.

What should you do if you or someone you know becomes a victim of financial exploitation or another form of elder abuse?

In most instances of suspected elder abuse, including financial exploitation, you should contact Adult Protective Services, generally a part of your county or state department of social services. You can find information about reaching your local Adult Protective Services office at the Eldercare Locator at **eldercare.acl.gov**, a public service provided by the U.S. Administration for Community Living, or by calling 1-800-677-1116.

If the older person is in danger or you believe a crime has been committed, call 911 for an immediate response from the police.

For cases of identity theft, contact your local police and the Federal Trade Commission (FTC) at 1-877-438-4338 or **identitytheft.gov**. If the loss involves funds held in a financial institution, such as a bank or credit union, report the problem to the financial institution immediately. If the loss involves credit products, such as a credit card or loan, contact the creditor immediately.

Remember that you are often not responsible for credit card charges or payments out of your bank account if you did not authorize them.

For more information go to **consumerfinance.gov/askcfpb**.

You will find more information and resources at the end of this guide.

Common Types of Elder Financial Exploitation

This module doesn't cover all types of elder financial exploitation in depth. However, it does discuss the key points and give some general guidelines to help you identify fraud, scams and other types of financial exploitation and give tips to help you prevent it from happening. This guide also provides a list of resources that you can consult as the need arises.

Exploitation by a Fiduciary

A person who is named to manage your money or property is a fiduciary. He or she must manage your money and property for your benefit. Financial exploitation can occur when a fiduciary abuses that power.

The person you appoint as your fiduciary should be trustworthy and honest. Your fiduciary has four basic duties:

1. Act only in your interest
2. Manage your money and property carefully
3. Keep your money and property separate from his/hers
4. Keep good records

Your fiduciary should be trustworthy and honest.

Your fiduciary can be removed if he or she does not fulfill his/her obligations or duties. Fiduciaries can be sued and may be ordered to repay money. If elder financial exploitation is reported to the police or Adult Protective Services, the fiduciary could be investigated. If the fiduciary is convicted of stealing your assets, he or she can go to jail.

Power of Attorney

One way some older adults prepare for the possibility of diminished financial decision-making capacity is by making a power of attorney (POA) for finances. A power of attorney gives someone else legal authority to make decisions about money or property. That person—called the agent—can make decisions if the older adult is sick or injured.

Creating a POA is a private way to appoint a substitute decision maker and is relatively inexpensive. If you don't appoint an agent under a POA before your decision-making

ability declines, a family member or friend might have to go to court to have a guardian appointed – and that process can be lengthy, expensive, and public.

A POA does involve some risk. It gives someone else – your agent – a great deal of authority over your finances without regular oversight. POA abuse can take many forms:

- Your agent might pressure you for authority that you do not want to grant.
- Your agent may spend your money on him or herself rather than for your benefit.
- Your agent might do things you didn't authorize him or her to do – for example, make gifts or change beneficiaries on insurance policies or retirement plans.

POAs differ

POAs vary, depending on what your state law allows and the wording in the document. Generally, a POA goes into effect as soon as it is signed unless the document specifies a different arrangement. That means that even if you are capable of making decisions, your representative can immediately act on your behalf.

There are ways to customize a power of attorney to fit your needs and preferences.

A durable power of attorney remains effective even if the grantor loses the capacity to make financial decisions. If you want your POA to remain effective if you become unable to manage your money or property, make sure it is durable.

There are ways to customize a power of attorney to fit your needs and preferences. An attorney can help you make an appropriate POA for your circumstances.

What are some ways to minimize the risk of POA abuse?

- Trust, but verify. Only appoint someone you really trust and make sure they know your wishes and preferences. You can require in your POA that your agent regularly report to another person on the financial transactions he or she makes on your behalf.
- Avoid appointing a person who mismanages their own money or has problems with substance abuse or gambling.
- Tell friends, family members, and financial advisers about your POA so they can look out for you.
- Ask your financial institution about its POA procedures. The financial institution may have its own form that it wants you to complete. But a POA that is valid under your state's law should be accepted by financial service providers.
- Remember that POA designations are not written in stone – you can change them. If you decide that your agent isn't or is no longer the best person to handle your finances, you can revoke (cancel) your POA. Notify your financial institution if you do this.
- Avoid appointing hired caregivers or other paid helpers as your agent under a power of attorney.
- Beware of someone who wants to help you out by handling your finances and be your new "best friend." If an offer of help seems too good to be true, it probably is.

Plan ahead!

A durable power of attorney is a very important tool in planning for financial incapacity due to Alzheimer's disease, other forms of dementia, or other health problems. It is advisable to consult with an attorney when preparing a power of attorney, a trust or any legal document giving someone else authority over your finances.

Help your agent under a power of attorney or other fiduciary help you.

The CFPB has plain language guides to help people acting as fiduciaries in three ways:

- The guides walk fiduciaries through their duties.
- The guides tell fiduciaries how to watch out for scams and financial exploitation, and what to do if their loved one is a victim.
- The guides tell fiduciaries where to go for help.

Guides are available to download or order free copies on the CFPB website.

The guides are available to download and you can order free copies on the CFPB website at **consumerfinance.gov/msem**.

If you or a loved one is a victim of financial exploitation by a fiduciary, take action immediately and make a report to Adult Protective Services or your local law enforcement agency.

Exploitation by Caregivers and In-Home Helpers – Tips to Defend You at Home

Elder financial exploitation is often perpetuated by family members and other caregivers.

You can take steps to guard against financial exploitation by someone acting as a caregiver or in-home helper.

- Secure your private financial documents including checks, financial statements and credit cards and statements. Consider using a locked file cabinet.
- Require receipts for purchases made by helpers.
- Monitor bank accounts and telephone bills. Ask for help from a third party, if needed, and consider an automatic bill pay system. Consider setting up transaction alerts that are monitored by a family member or other third party.
- Do not let hired caregivers or helpers open your mail, pay your bills, or manage your finances.
- Never promise money or assets to someone when you die in exchange for care provided now.
- Never lend employees money or personal property.
- If you have trouble reading your statement, ask your financial institution if a second copy of your statement can go to someone who can read it for you. This person does not need to have authority to act on your behalf. Also, your financial institution may be able to send you your statement in large print.
- Never let caregivers use your credit/debit card to run errands or make purchases for you.
- Secure your valuables such as jewelry and other property.
- Check your free credit reports at **annualcreditreport.com**.

Romance Scams

A romance scam is when a new love interest says they love you, but they just want your money. And the person may not be who they say they are. Romance scams can happen online or in person.

Romance scams are on the rise, according to new Federal Trade Commission data that show consumers reported losing a record $304 million to the scams in 2020. The amount consumers reported losing to romance scammers is up about 50 percent since 2019 and has increased over 400 percent since 2016.

Online romance scams

Online romance scammers can connect with people through social media, dating apps, websites, text messages, or email. They may draw people into a relationship by building false personas that seem just real enough to be true. They may use their own photos or steal other people's photos from the Internet. Romance scammers often get information from social media profiles so they can fake similar interests, hobbies, and values.

Eventually, the supposed suitor will ask for money in a variety of ways. They may start small by asking for a small monetary loan for a car repair or help paying a medical bill to gauge the willingness to lend money. After the first few successful asks, the loan amounts may become higher. They also may ask for gift cards or wire transfers, which are hard to trace. Some scams may involve identity theft, misuse of government benefits, or even money laundering. The median loss reported to the FTC for romance scams is $2,500—over 10 times higher than the median loss across all other frauds.

The social and physical distance recommendations associated with the COVID-19 pandemic has led to loneliness and isolation, and romance scammers are taking advantage of people's need

for connection. Scammers may even use a natural disaster, pandemic, or other current events as an excuse not to meet in person, which could keep their online scam going.

In person romance scams

Some romance scams happen in person. This financial exploitation could involve older adults who are socially isolated or dependent on others to assist them. The scammer could be a person you meet at places such as your church, community center, or social group.

Romance scammers may take time to build trust with you. They may ask for a small monetary loan at first, and increase the amount based on willingness to lend money.

Warning signs

Online and in-person romance scammers are financial predators. They play to your affection to gain your trust and access to your money. Here are some warning signs:

A new friend or love interest may:

- be overly complimentary and flirtatious;
- shower you with affection and overwhelm you with texts, emails, and phone calls;
- suggest or insist that you keep the "relationship" a secret;
- pressures or hurries you to share your private financial information or seem pushy or nosy about your finances.

Online romance scammers often say they can't visit you in person because they are:

- living or traveling outside of the country
- working on an oil rig
- in the military
- a doctor with an international organization

Romance scammers:

- claim to need money for an emergency surgery or other medical bills
- ask for a loan or gift by wire transfer, gift cards or even cash.
- say they need to pay customs fees or gambling debts
- request money for plane ticket or other travel expenses, a visa or other official travel documents

Getting help:

If you think you are being scammed or have given, or sent, money to a scammer:

- Stop communicating with the person;
- Notify your financial institution immediately If you sent money or gave someone your banking information;
- Talk to someone you trust (a family member, friends or clergy). If they say they are concerned about your new love interest, pay attention!
- Report local in-person romance scams to local law enforcement and Adult Protective Services (APS);
- Report online romance scams to FBI's Internet Crime Complaint Center;
- Report all scams to the Federal Trade Commission at **reportfraud.ftc.gov**

The sooner you act and report scams, the better the chance you'll have of intercepting any stolen funds.

Investment Fraud

Investment Fraud (also known as Securities Fraud) is a term that covers a wide range of illegal activities including the deception of investors or the manipulation of financial markets.

We've all heard the timeless saying "If it sounds too good to be true, it probably is." As an investor, these are good words to live by. The trick is knowing when "good" becomes "too good."

Senior certifications and designations

A popular practice among financial services salespeople is to identify themselves by a "senior designation" to signal that they have expertise in retirement planning or the investment needs of older people.

The requirements to earn and maintain financial credentials, such as a senior designation, vary considerably. Programs of study range from weekend seminars to two-year graduate programs. The initials on a business card don't provide information about the quality of the designation. Some designations indicate extensive knowledge in the financial needs of older consumers, while others are merely marketing tools.

While the majority of investment advisers, financial planners, and broker-dealers are honest and reputable, it pays to check on a senior designation if you are presented with one (see details on page 23). Be wary of investment scams, including the ones listed on the next page.

Common investment scams

- **Ponzi schemes:** This is an old scam with a simple formula: Scammers promise high returns to investors. Money from new investors is used to pay previous investors. These schemes eventually collapse—leaving most of the investors with a financial loss.
- **Unscrupulous financial advisers:** Some advisers cut corners, resort to outright fraud, or bilk older adults with unexplained fees, unauthorized trades or other irregularities.
- **Affinity fraud:** A scammer pretends to be a member of a religious organization or a military or an ethnic group in order to win the trust of a member or members of the

group. Those committing affinity fraud often use symbols, language, and iconography to appear associated with a specific group in their solicitations.

- **Internet fraud – the "Dot-Con":** Using the internet, it is easy for con artists to reach millions of potential older victims at minimal cost. This form of fraud is constantly evolving. Scammers often design email and social media accounts to appear as legitimate businesses or even family members.
- **Inappropriate or fraudulent annuity sales:** Variable annuities are often pitched to seniors through "free lunch" investment seminars. These products can be unsuitable for many retirees and are sometimes sold by salespersons who fail to disclose steep sales commissions and surrender charges that impose costly fees or penalties for taking the money out before the maturity date.

How do I check the credentials of my financial adviser?

You can check a broker's background via the Financial Industry Regulatory Authority (FINRA) BrokerCheck at **finra.org** or by calling the FINRA BrokerCheck Hotline at 1-800-289-9999.

You can check the background of a Registered Investment Advisor via the Securities and Exchange Commission (SEC) Investment Advisor Public Disclosure Database at **adviserinfo.sec.gov**. You may also contact your state securities office and Better Business Bureau to check if there have been any disciplinary actions against a licensed securities broker/dealer.

To learn more about senior certification and designations, visit FINRA at **finra.org/investors/professional-designations/accredited-designations**. Scroll to the bottom of the FINRA page to find links to other helpful resources.

Consult the CFPB consumer guide *Know Your Financial Adviser* to help you ask the right questions if you're shopping for an adviser with expertise in senior financial planning. Visit **consumerfinance.gov/blog/know-your-financial-adviser**.

Loss prevention tips for investors

Invest wisely online and offline. Here are some important tips you should keep in mind when you are considering purchasing investment products and for protecting those investments once you have them:

- Never judge a person's trustworthiness by the sound of their voice.
- Take your time when making investment choices. Be careful of "act now" or "before it's too late" statements.
- Say "no" to anybody who tries to pressure you or rush you into an investment.
- Be wary of salespeople who prey upon your fears or promise returns that sound too good to be true, such as guaranteed high interest rates or no risk investments.
- Always ask for a written explanation of any investment opportunity and then shop around and get a second opinion.
- Be wary of any financial adviser who tells you to leave everything in his or her care.
- Stay in charge of your money or enlist the help of a trusted and capable third party to assist you.
- Make checks payable to a company or financial institution, never an individual.
- Retain and maintain account statements and confirmations you receive about your investment transaction.

- Document every conversation with financial advisers.
- Don't put all of your eggs in one basket—divide your investments among different asset categories, such as stocks, bonds, and cash held in federally insured deposit accounts.
- Take immediate action if you detect a problem. Time is critical, so do not be afraid to complain.
- Don't let embarrassment or fear stop you from reporting financial exploitation or investment fraud.

Additional tips to keep in mind when considering investment products

- Save enough emergency money in a savings or other readily accessible federally insured deposit account to support you and your family for at least six months before investing in non-deposit products.
- Do your homework. Never invest in a product you do not understand fully.
- Attend classes, seminars, or check the business reference section of the public library to become better informed.

Understand the risks before investing. Investments always have some degree of risk.

- Look out for marketing techniques. Many investment professionals offer "free meal seminars" as a marketing technique for obtaining new clients. Check the background of the presenter, research any recommended investment products, and get a second opinion before making the decision to invest. That "free meal seminar" can turn out to be expensive if it results in your becoming a victim of fraud.

- Understand the risks before investing. Investments always have some degree of risk.
- Tell your financial adviser of your financial objectives and risk tolerance.

Understanding FDIC insurance

If you select investment products offered by a bank, it is important to understand which of your investments are covered by the Federal Deposit Insurance Corporation (FDIC). The FDIC insures funds in deposit accounts at FDIC-insured institutions including:

- Checking
- Savings
- Money Market Deposit Accounts (MMDAs)
- Certificates of Deposit (CDs)

Another federal agency, the National Credit Union Administration, provides similar deposit insurance coverage to depositors at federally insured credit unions.

FDIC insurance protects depositors up to a capped amount in the event of a bank failure. It does **not** protect depositors from losses resulting from theft, fraud, or robbery.

FDIC does not insure non-deposit investment products, even if they were purchased at an insured bank, including stocks, bonds, mutual fund shares, life insurance policies, annuities and municipal securities. When you meet or talk with a sales representative about non-deposit investment products, they must tell you that the product(s) are not insured by the FDIC.

Contents of safe deposit boxes also are not protected by FDIC insurance.

By law, federal deposit insurance is backed by the full faith and credit of the federal government. If a bank fails, the FDIC will pay all insured deposits up to the insurance limit, including principal and any accrued interest through the date of the bank closing. Federal law requires that all insured deposits be paid as soon as possible.

Insurance coverage and ownership categories

Deposit insurance coverage is based on a depositor's ability to meet the specific requirements for an ownership category. The most common account ownership categories for individual and family deposits are single accounts, joint accounts, revocable trust accounts, and certain retirement accounts.

Each ownership category has different requirements, and the potential amount of insurance coverage for each category is based on the Standard Maximum Deposit Insurance Amount (SMDIA), which is $250,000.

For additional details on the coverage limits, requirements, and in-depth information on all account ownership categories and other types of deposit accounts, visit **fdic.gov/deposit/deposits**, call toll-free 1-877-ASK-FDIC (1-877-275-3342), or talk to your bank representative.

Avoiding Telephone and Internet Scams

Older adults are increasingly the targets of scam artists on the telephone who use lies, deception, and fear tactics to convince the older adult to send them money or provide personal account information. The Do-Not-Call registry may reduce calls from telemarketers representing legitimate businesses; however, it will not stop criminal telemarketers from calling.

Grandparent Scam

An example of a common telephone scam is the "grandparent scam". In this scenario, an imposter calls a grandparent pretending to be a grandchild in trouble. The scammer may even know the grandchild's name. The scammer is usually crying, making it hard to recognize the grandchild's voice. The scammer pleads for the grandparent to immediately wire money and not tell any family members for fear of upsetting them. Many people will immediately jump to the assistance of the grandchild and won't ask questions until later. Scammers also know that many older people may have experienced a hearing loss and won't detect any differences from their grandchild's voice. Or they may attribute the differences they do hear to the stress of the situation.

IRS Telephone Scam

According to the Internal Revenue Service (IRS), in this telephone scam, a scammer calls telling the consumer that he or she must immediately pay taxes that are owed. In some cases, the scammers target immigrants, who are told that if they don't pay the tax bill or otherwise follow instructions, they will face serious consequences, such as arrest and deportation, or that the IRS could shut off their utilities or revoke their driver's licenses. Callers are frequently insulting or hostile to scare their potential victims.

These scammers frequently:

- Tell potential victims that they are entitled to big refunds, or that they owe money that must be paid immediately to the IRS. When unsuccessful, they often call back trying new strategies.

- May spoof the IRS toll-free number on caller ID to make it appear that it's the IRS calling.
- Use common names and surnames to identify themselves and fake IRS badge numbers.
- May know the last four digits of a victim's Social Security number.
- Send bogus IRS emails to victims to support their bogus calls.
- Create background noise to mimic a call site.
- Threaten jail time or driver's license revocation.
- Hang up and call back pretending to be from the local police or DMV (with fake caller ID to trick the victim into believing that it is an official call) and threaten the victim with arrest or revocation of his/her driver's license.

The IRS never asks for credit card, debit card or prepaid card information over the telephone.

For more information from the IRS on this type of scam, go to **irs.gov/newsroom/tax-scams-consumer-alerts**.

The IRS has warned that this crime continues year round. The IRS will always send taxpayers a written notification of any tax due via the U.S. mail. The IRS never asks for credit card, debit card or prepaid card information over the telephone. And the IRS does not initiate contact with taxpayers by email, text message, or through social media to request personal or financial information such as PINs or passwords, credit card, bank or other accounts.

If you get a **phone call** from someone claiming to be from the IRS, here's what you should do:

- If you know you owe taxes or you think you might owe taxes, call the IRS at 1-800-829-1040. The IRS employees at that line can help you with a payment issue, if there really is such an issue.

- If you know you don't owe taxes or have no reason to think that you owe any taxes (for example, you've never received a bill or the caller made some bogus threats as described above), or if you think the party who called you is not really with the IRS, then call and report the incident to the Treasury Inspector General for Tax Administration at 1-800- 366-4484.
- You can also report the suspected scam by going to **irs.gov/privacy-disclosure/report-phishing**.
- You can file a complaint using the FTC Complaint Assistant at **ftccomplaintassistant.gov**; choose "Scams and Rip-offs" and then "Imposter Scams."

If you get an **email** from someone claiming to be from the IRS, don't open any attachments or click on any links contained in the message. Instead, report it to the Treasury Inspector General for Tax Administration at **treasury.gov/tigta** and forward the e-mail to **phishing@irs.gov** with the subject "IRS Phone Scam."

More information on how to report phishing scams involving the IRS is available on the IRS website, **IRS.gov**.

Lottery and Sweepstakes Scams

Sweepstakes scammers call, email, or text consumers congratulations on winning a lottery, drawing, or sweepstakes, which the consumers usually have not even entered. The scammer asks the "winner" for an upfront payment to cover processing fees or taxes. In another variation, the scammers send a letter with an authentic-looking, but phony "Claim Certificate" or "check" as an advance to pay the winnings. Bankers are generally aware of this scam and how to spot the phony checks. But if you deposit a phony check, the financial

institution might hold you responsible for repayment of the entire amount of the fraudulent check even if you sent some of the money to the scammer.

Sweepstakes Recovery Scam

Once it is apparent that no winnings are forthcoming, the victim may receive another call from a person claiming to be an attorney representing sweepstakes winners. In exchange for an upfront fee, the so-called "attorney" offers to collect the winnings on behalf of the victim. Needless to say, the "attorney" is actually an associate of the original scammer and there is no chance of recovering the original loss or the fraudulent fee that the fake "attorney" charges.

Tips for Avoiding Telephone Scams

Scammers can be very convincing. If something seems unusual, check it out.

- You usually cannot win a sweepstakes or a lottery that you did not enter.
- Never "pay to play." A legitimate sweepstakes will not ask for money upfront.

If something seems unusual, check it out.

- Be suspicious of any pressure to send funds via wire transfer or a pre-paid reloadable card.
- Pay attention to warnings from your financial institution telling you that a request sounds like a scam. Your banker may have encountered similar scams in the past.
- Scammers often claim an emergency, hoping you will respond quickly without checking out the situation first. Before offering your help to someone who claims to be a

grandchild (or any other relative/friend), be sure to telephone your grandchild or his/her parents at a number you know to be valid to find out if the request is legitimate. If a caller claims to be from an established organization such as a hospital, a charity, or a law enforcement agency, look up the number of the organization yourself.

- Consider it a red flag if the caller insists on secrecy. Never allow anyone to discourage you from seeking information, verification, support and counsel from family members, friends or trusted advisers before you make a financial transaction.

ACTIVITY 1: Telephone Scams

Read each scenario and then, based on what you have learned, answer the questions in the spaces provided:

SCENARIO 1 Jane is home watching TV when the telephone rings. She answers the call and the man on the line says "Congratulations! You've won $2.7 million dollars in the lottery!" Jane is surprised. Although she buys lottery tickets, she hasn't given her name to anyone. The caller tells her that there are a couple of things she needs to do before she can receive her check. He directs Jane to go to her bank and withdraw $2,700 to cover processing fees. He tells her to forward the funds through a local wire service or to buy and send a special prepaid card that will expedite the process. Jane heads to her bank to withdraw the money. The next day the person calls to say they received the funds and an additional $5,000 is needed to pay the taxes.

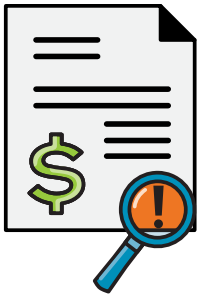
QUESTION: What were the red flags that should have warned Jane that she was about to become a victim of a scam?

SCENARIO 2 A few weeks after Jane used a pre-paid card to transfer money to the scammer, she received a call from a person claiming to be an attorney representing sweepstakes winners. The attorney offered to recover the winnings for Jane but she would have to pay him a $7,000 fee up front.

QUESTION: What should Jane do?

SCENARIO 3 Jack lives alone in his home of 40 years. He has become increasingly hard of hearing, which has made it difficult for him to communicate on the telephone. One afternoon he receives a call from a distressed-sounding person who says "Hi Grandpa, this is your favorite grandson." When Jack asks "is this Johnny?" the caller says "yes grandpa, it's Johnny." Johnny says he's in Canada and has been arrested. Johnny explains that he needs Jack to wire $2,500 to bail him out. Johnny also says "please don't tell Mom – I don't want her to get upset." Jack hurries to his bank and insists on wiring the money despite warnings from the teller and the bank manager that this sounds like a scam.

QUESTION: What are the red flags in this story?



Phantom Debt Collection Scam

Scam debt collectors try to trick their victims into paying a debt that doesn't exist. These phony debt collectors often contact older adults by phone and refuse to answer questions about themselves and the underlying debt. Phony debt collectors may have some information about the older person that they'll use to appear to be legitimate. Scam debt collectors may use scare tactics and may threaten to do things that they can't do, such as threatening to arrest the older person or physically hurting him or her unless the debt is paid immediately.

Other characteristics of this scam may include:

- You don't recognize the debt, and the debt collector refuses to give you information about the debt.
- The debt collector refuses to give you a mailing address or phone number.
- The debt collector claims that it can press criminal charges against you if you refuse to pay the debt collector immediately.
- The debt collector asks you for sensitive personal financial information.
- The debt collector asks you to use an anonymous way to pay, such as buying and sending a pre-paid debit card, providing a pre-paid card number over the phone, or using a wire transfer or an electronic transfer from your bank account.

How to respond to a possible debt collection scam

If you receive a call from someone claiming to be a debt collector, ask for more information. Don't ignore your suspicions if you don't recognize the debt, and don't give in to threats.

- Ask the caller for his or her name, company, street address, and telephone number.
- Request an explanation of the debt in writing, including information about any interest, fees or charges added to the original amount, the name of the original creditor, and how to dispute the debt.

- Depending on your situation, there are different ways to respond to common problems you may experience with real debt collectors.
- Sample letters you can use to respond to debt collectors can be found at **consumerfinance.gov/consumer-tools/debt-collection**.
- If you can't verify the information the collector provides, do not give money or your financial information (such as a bank account number or credit card number) to the caller or company.
- Don't give the caller your financial or other personal information such as your social security number or date of birth.
- It's a good idea to keep the letters or documents a debt collector sends you, and keep copies of anything you send to a debt collector. You can also write down dates and times of conversations along with notes about what you discussed. These records can help you remember, or show others what actually happened.

ACTIVITY 2: Phantom/Scam Debt Collection

Read the scenario and then, based on what you have learned, answer the questions in the space provided:

SCENARIO Pamela is sitting down to eat when she receives the sixth call of the day from a phone number that she doesn't recognize. Pamela usually doesn't answer the phone unless she recognizes the number because she is wary of scams.
Pamela doesn't pick up the phone. The caller leaves a voice message stating that Pamela owes $349 to Federal Collections, Inc. The message says that if Pamela doesn't pay $349 by 11:00 a.m. tomorrow, a warrant will be issued for her arrest. Pamela would feel humiliated if she were arrested in front of her neighbors. She picks up the phone.

The caller tells Pamela that she can avoid being arrested by wiring $349 through a money transfer.

QUESTION: What are the red flags that should warn Pamela that this is a scam?

QUESTION: If you were Pamela, what would you do?

Avoiding Charity Scams

If you're considering a request for a donation to a charity, do some research before you give. By finding out as much as you can about the charity, you can avoid fraudsters who try to take advantage of your generosity. Here are tips to help make sure your charitable contributions don't go to a scammer. For more information, visit **ftc.gov/charityfraud**.

Signs of a Charity Scam

According to the Federal Trade Commission (FTC), charities and fundraisers (groups that solicit funds on behalf of organizations) use the phone, face-to-face contact, email, the internet (including social networking sites), and mobile devices to solicit and obtain donations. Naturally, scammers use these same methods to take advantage of your goodwill. Regardless of how they reach you, be cautious of any charity or fundraiser that:

- Refuses to provide detailed information about its identity, mission, costs, and how the donation will be used, including what percent of your donation will go to the charity rather than to the caller or the caller's company.
- Doesn't provide proof that a contribution is tax deductible.
- Uses a sound-alike name that closely resembles that of a better-known, reputable organization.
- Thanks you for a pledge you don't remember making.
- Uses high-pressure tactics such as trying to get you to donate immediately, without giving you time to think about it and do your research.
- Asks for donations in cash or asks you to wire money.
- Offers to send a courier or overnight delivery service to collect the donation immediately.
- Guarantees sweepstakes winnings in exchange for a contribution. By law, you never have to give a donation to be eligible to win a sweepstakes.

Charity Checklist

These precautions can help you ensure that your donation benefits the people and organizations that you want to help.

- Ask for detailed information about the charity, including name, address, and telephone number.
- Get the exact name of the organization and do some research. Searching the name of the organization online — especially with the word "complaint(s)" or "scam" — is one way to learn about its reputation.
- Call the charity directly. Find out if the organization is aware of the solicitation and has authorized the use of its name. The organization's development staff should be able to help you.

Keep a record of your donations.

- Find out if the charity or fundraiser must be registered in your state by contacting the National Association of State Charity Officials **nasconet.org**.
- Check on the charity by contacting the Better Business Bureau's (BBB) Wise Giving Alliance at **give.org** or **guidestar.org**.
- Ask if the caller is a paid fundraiser. If so, ask:
  - The name of the charity they represent
  - The percentage of your donation that will go to the charity
  - How much will go to the actual cause to which you're donating
  - How much will go to the fundraiser
- Keep a record of your donations.

- Make an annual donation plan. That way, you can decide which causes to support and which reputable charities should receive your donations.
- Use the IRS Exempt Organizations Select Check at **apps.irs.gov/app/eos** to find out which organizations are eligible to receive tax deductible contributions.
- Know the difference between "tax exempt" and "tax deductible." Tax exempt means the organization doesn't have to pay taxes. Tax deductible means you can deduct your contribution on your federal income tax return.
- Never send cash donations. For security and tax purposes, it's best to pay by check — made payable to the charity — or by credit card.
- Never wire money to someone claiming to be a charity. Scammers often request donations to be wired because wiring money is like sending cash: once you send it, you can't get it back.
- Do not donate until you've thoroughly researched the charity.

Never wire money to someone claiming to be a charity.

- Be wary of charities that spring up suddenly in response to current events and natural disasters. Even if they are legitimate, they may not have the infrastructure to get the donations to the affected area or people.
- If a donation request comes from a group claiming to help your local community (for example, local police or firefighters), ask the local agency if they have heard of the group and are getting financial support.

- What about texting? If you text to donate, the charge will show up on your mobile phone bill. If you've asked your mobile phone provider to block premium text messages — texts that cost extra — then you won't be able to donate this way.

Charities and the Do Not Call Registry

The National Do Not Call Registry gives you a way to reduce telemarketing calls from legitimate businesses, but it exempts charities and political groups. However, if a fundraiser is calling on behalf of a charity, you can tell them to stop calling you. If the calls continue, the fundraiser may be subject to a fine. To sign up for the Registry, verify a registration or submit a complaint, go to **donotcall.gov**.

Report Charity Scams

If you think you've been the victim of a charity scam or if a fundraiser has violated Do Not Call rules, file a complaint with the Federal Trade Commission. Your complaints can help detect patterns of wrong-doing and lead to investigations and prosecutions.

Computer/Internet Scams

Phishing and **spoofing scams** can dupe older adults into giving out their personal financial information. Phishing scammers create authentic-looking emails, text messages, and/or internet pages to entice their victims into disclosing financial information such as credit card details, bank or credit card account numbers, Social Security numbers, Medicare numbers, etc.

Here are some examples:

- "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."
- "During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."
- "Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."

The messages may appear to be from organizations you do business with–such as your financial institution or your insurance company. They may even threaten to close your account or take other action if you don't respond.

The senders are "phishing" for your private account information so they can use it to commit fraud or identity theft against you.

Scammers disguise or "spoof" an email address to make it look like it is coming from someone you may know. For example, you may receive an email that looks like it is coming from a friend who needs money to deal with an emergency.

In another twist, scam artists are using the phone to try to break into your computer. They call, claiming to be computer techs associated with well-known companies. They say that they've detected viruses or other malware on your computer to trick you into giving them remote access or paying for software you don't need. These scammers take advantage of your reasonable concerns about viruses and other threats. They know that computer users have heard that it is important to install security software. But the purpose behind their elaborate scheme is not to protect your computer; instead, they are trying to install malware to steal passwords and account numbers.

Tips for avoiding computer or internet scams

Take precautions with your personal computer (PC) to reduce your risk of a computer/internet attack:

- Use trusted security software and make sure it's updated regularly.
- Do not email financial information or account numbers. Email is not a secure method of transmitting personal information.
- Be cautious about opening attachments and downloading files from emails, regardless of who sent them. These files can contain viruses or other malware that can compromise your computer's security.

Be cautious about opening attachments and downloading files from emails, regardless of who sent them.

- Use passwords that will be hard for hackers to guess. For example, use a mix of numbers, symbols, and capital and lower-case letters instead of easily guessed words.
- Shut down your PC when you are not using it.
- Don't give control of your computer to a third party who calls you out of the blue.
- Do not rely on caller ID alone to authenticate a caller. Criminals spoof caller ID numbers. They may appear to be calling from a legitimate company or a local number, when they're not even in the same country as you.
- Online search results might not be the best way to find technical support or get a company's contact information. Scammers sometimes place online ads to convince you to call them. If you want tech support, look for a company's contact information on the software package or on your receipt.

For practical tips to help you guard against internet fraud, secure your computer, and protect your personal information, visit **OnGuardOnline.gov**. If you believe you are the victim of Internet crime, or if you are aware of an Internet crime, you can file a complaint with the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center at **ic3.gov.**

How to Respond to a Phishing Attack or a Tech Support Scam

Even if you use security software, chances are high that some questionable messages will get through. Some of these messages look very realistic. Here are some tips for protecting yourself.

- Do not open any message that comes from an unfamiliar source. If you open a suspicious message, delete it. Do not click on links or call telephone numbers provided in the message. Be wary about opening attachments.
- Delete email and text messages that ask you to confirm or provide personal information (credit card and bank account numbers, Social Security numbers, passwords, etc.). Legitimate companies do not ask for this information via email or text.
- If you're concerned about your account or need to reach an organization that you do business with, call the number on your financial statements or on the back of your credit card or in the telephone book. Do not call the telephone number that the caller or spoof website provides you!
- If you receive an email that looks like it is from a friend or relative asking you to send money, call them to verify that the email really came from them.

- If you think you might have downloaded malware from a scam tech support site, don't panic. Update or download legitimate security software and scan your computer. Follow the instructions of the security software to eliminate any problems. Change any passwords that you gave out. If you use those passwords for other accounts, change those passwords, too. If you paid for bogus services with a credit card, dispute the transactions with your credit card provider. Check your statements for any other charges you didn't make, and dispute those as well. For more information, go to **consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams**. If you believe you are the victim of Internet crime, or if you are aware of an Internet crime, you can file a complaint with the FBI's Internet Crime Complaint Center at **ic3.gov**.

Victims of phishing or tech support scams could become victims of identity theft. Act promptly to avoid financial loss or damage to your credit. You'll find more information and resources at the end of the following section on Identity Theft.

Identity Theft

Identity theft occurs when thieves steal your personal information (e.g., your Social Security number (SSN), birth date, credit card numbers, personal identification numbers (PINs), or passwords). With sufficient information, another person can use your identity to commit fraud or other crimes.

How to Avoid Identity Theft

- **Protect your Social Security number, credit card and debit card numbers, PINs, passwords, and other personal information.**
  Never provide this information in response to an unwanted telephone call, fax, letter, or email, no matter how friendly or official the circumstances may appear. Watch out for people who may be trying to look over your shoulder while you use the ATM, seeking to steal your personal identification number. In case your wallet is lost or stolen, carry only the identification you really need: checks, credit or debit cards. Keep the rest, including your Social Security card, in a safe place. Do not preprint your Social Security number, telephone number, or driver's license number on your checks. You do not have to give merchants your Social Security number; if requested, ask the merchant to use another form of identification that does not include your Social Security number (e.g., a passport or driver's license).

- **Protect your incoming and outgoing mail.**
  For incoming mail: Try to use a locked mailbox or other secure location (e.g., a post office box). If your mailbox is not locked or in a secure location, try to promptly remove mail that has been delivered or move the mailbox to a safer place. When ordering new checks, ask about having the checks delivered to your bank branch instead of having them mailed to your home where you run the risk of a thief finding them outside your front door.

  For outgoing mail containing a check or personal information: Try to deposit it in a United States (U.S.) Postal Service blue collection box, hand it to a mail carrier, or take it to the post office instead of leaving it in your doorway or home mailbox. A mailbox that holds your outgoing bills is a prime target for thieves who cruise neighborhoods looking

for account information. Avoid putting up the mailbox flag to indicate that outgoing mail is waiting.

- **Sign up for direct deposit.**
  Sign up for direct deposit of your paycheck, retirement check, and/ or state or federal benefits, (e.g., Social Security). Direct deposit prevents someone from stealing a check out of your mailbox and forging your signature to access your money. Direct deposit is also beneficial in the event of a disaster.
- **Keep your financial trash "clean."**
  Thieves known as dumpster divers search through garbage looking for pieces of paper containing Social Security numbers, bank account information, and other details they can use to commit fraud. What is your best protection against dumpster divers? Before tossing out these items, destroy them, preferably using a crosscut shredder that turns paper into confetti that cannot be easily reconstructed.

Contact your financial institution immediately if there is a discrepancy in your records or if you notice something suspicious.

- **Keep a close watch on your bank account statements and credit card bills.**
  Monitor these statements each month and contact your financial institution immediately if there is a discrepancy in your records or if you notice something suspicious (e.g., a missing payment or an unauthorized withdrawal). Contact your institution if a bank statement or credit card bill does not arrive on time. Missing financially related mail could be a sign someone has stolen your mail and/ or account information, and may have changed your mailing address to run up bills in your name from a phony location.

- **Avoid come-ons for personal information on the internet.** As was mentioned in the section on Computer/Internet Scams, never provide bank account or other personal information in response to an unsolicited email, telephone call, text message or when visiting a website that does not explain how personal information will be protected. Legitimate organizations would not ask you for these details because they already have the necessary information, or can obtain it in other ways. If you believe the correspondence is fraudulent, consider bringing it to the attention of the Federal Trade Commission (FTC) via its online complaint form: **ftccomplaintassistant.gov**.

  If you do open and respond to a phony email, contact your financial institution immediately and follow the steps listed in the FTC brochures listed at the end of this guide. For more about avoiding phishing scams, visit **consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams**.

- **Review your credit report annually (every 12 months) and report fraudulent activity.** Review your credit report carefully for warning signs of actual or potential identity theft. For example, items that include mention of a credit card, loan, or lease you never signed up for, or requests for copies of your credit report from someone you do not recognize could be a sign that a con artist is snooping around for personal information. To obtain a free copy of your credit report, visit **annualcreditreport.com.**

You can submit a complaint about problems with credit reporting companies or information about your credit reports to the CFPB at **consumerfinance.gov** or 1-855-411-2372. For more information: **consumer.ftc.gov/blog/2017/09/fraud-alert-or-credit-freeze-which-right-you** or Ask CFPB at **consumerfinance.gov/askcfpb.**

Fraud Alert: Social Security Administration

The Inspector General for the Social Security Administration (SSA) is warning the public, and Social Security beneficiaries in particular, to be aware of fraud scams that target personal information.

In the most recent scam, identity thieves obtain the personal information of Social Security beneficiaries and use that information to attempt to open a counterfeit "my Social Security" online account on SSA's website **ssa.gov**. If successful, they then use that account to redirect the beneficiary's direct deposit benefits to an account controlled by the thief.

Protect your personal information as you would any other thing of value.

This should not discourage people from using SSA's "my Social Security" feature, which enables the public to set up an online account to view earnings history and estimated benefits, and allows beneficiaries to obtain a host of services online. Establishing your "my Social Security" account yourself eliminates the risk of a phony account being opened by an identity thief. This type of crime does, however, serve as a reminder to protect your personal information as you would any other thing of value. Once thieves have your personal information, they can use it to open credit accounts, buy homes, claim tax refunds, and commit other types of costly fraud.

If you receive information from SSA indicating that you have opened a "my Social Security" account, and you did not open the account, you should contact Social Security promptly so that appropriate action may be taken, and the matter may be referred to the Office of the Inspector General. You can do so by visiting or calling a local SSA office or calling SSA's toll free customer service at 1-800-772-1213. Individuals who are deaf or hearing-impaired can call Social Security's TTY number at 1-800-325-0778.

Identity Theft: If You Think You May Be a Victim

If you believe you are a victim of identity theft, the FTC recommends that you immediately take the following actions:

- Place an initial fraud alert with one of the three nationwide credit reporting companies.
- Order your credit reports and review for incorrect information or new, unauthorized account activity.
- Create an identity theft report.
- Consider placing an extended fraud alert or security freeze on your credit report to limit the circumstances under which a credit reporting company may release your credit report.

The FTC has many resources available to help you. Call the FTC's Identity Theft Hotline at 1- 877-IDTHEFT (438-4338) or visit **identitytheft.gov**. Its online toolkit includes:

- A detailed guide for protecting your information, with instructions and sample letters to help identity theft victims.
- Sample letters to help you dispute unauthorized charges or the opening of new accounts in your name. Sample letters and forms are available at **identitytheft.gov/Sample-Letters.**

Medical Identity Theft

Medical identity theft is serious business. According to one study, about 1.5 million adults are victims of medical identity theft each year.

What Is Medical Identity Theft?

Medical ID theft occurs when someone steals personal information — such as your name and Medicare number — and uses the information to get medical treatment, prescription drugs, surgery and/or other services and then bills Medicare for it.

A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file phony claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, or credit report may be affected.

Every time a thief uses your identity to get care, a record is created with incorrect medical information about you.

If you see signs of medical identity theft, order copies of your records and check for mistakes. You have the right to correct these mistakes.

Medical ID theft can cause financial harm but it is about more than just losing time and money. Sometimes people are denied Medicare coverage for a service or medical equipment because their records falsely show they already received it, when in fact it went to someone posing as them.

It can affect your medical and health insurance records. Every time a thief uses your identity to get care, a record is created with incorrect medical information about you. That information might include:

- A different blood type
- An inaccurate history of drug or alcohol abuse
- Test results that are not yours

- A diagnosis of an illness, allergy or condition that you do not have, which could lead to you receiving the wrong treatment and even being injured or getting sick due to an incorrect treatment.

All types of people, including doctors and medical equipment companies, have been caught stealing people's medical identities. There have even been links to the mafia and thieves in other countries. Sadly, about one-third of medical identity thieves are family members.

How Do You Learn if You Are a Victim?

Here are some warning signs that your identity may have been stolen:

You are denied insurance for a medical condition you do not have.

- You get a bill for medical services you did not receive.
- You are contacted by a debt collection company for money you do not owe.
- Your insurance company says you've reached your limit on medical benefits.
- You are denied insurance for a medical condition you do not have.

How to Avoid Medical Identity Theft

- Protect your Medicare and other health insurance cards in the same way you would protect a credit card.
- Review your Medicare Summary Notices (MSN), Explanations of Benefits (EOB) statements and medical bills for suspicious charges. If you find incorrect information in your records, insist that it be corrected or removed.
- Only give personal information to Medicare-approved doctors, other providers and suppliers, your State Health Insurance Assistance Program or Senior Medicare Patrol (SMP) program, or the Social Security Administration. Call 1-800-MEDICARE (1-800-633-4227) if you aren't sure if a provider is approved by Medicare.
- Beware of offers of free medical equipment, services or goods in exchange for your Medicare number.
- Shred papers with your medical identity before putting them in the trash.
- Remove or destroy labels on prescription bottles and packages before you put them in the trash.

Remove or destroy labels on prescription bottles and packages before you put them in the trash.

How to Respond if You Suspect Medical Identity Theft

- Ask your health care provider for a copy of your current medical file. If anything seems wrong, write to your health plan or provider and ask for a correction.
- Contact your local Senior Medicare Patrol (see contact information below).

How Your Senior Medicare Patrol (SMP) Can Help

Your local SMP is ready to provide you with the information you need to protect yourself from Medicare errors, fraud and abuse, detect potential errors, and report your concerns. For more information or to locate your state SMP go to **smpresource.org**.

ACTIVITY 3: Identity Theft Self-Check

Review each response on the list and indicate whether you perform this action always, sometimes, or never. Then, tally your score and see how well you are taking measures to avoid identity theft.

	Always 2 points	Sometimes 1 point	Never 0 points
1. Cover or block the Point of Service (POS)/ATM keypad when I enter my PIN			
2. Carry only the identification, checks, credit cards, or debit cards I really need			
3. Use direct deposit for paychecks, tax refunds, benefits payments, etc.			
4. Shred documents with personal/financial information before disposing of/recycling them			
5. Use complex passwords with a mix of numbers, symbols, and letters instead of easily guessed words			
6. Review financial statements/bills monthly and identify/correct errors			
7. Review my credit report annually and identify/correct errors			
8. Use secure mailboxes for incoming/outgoing mail			
9. Avoid providing/sharing personal information (e.g., SSN) whenever possible			
10. Review my Medicare Summary Notices (MSN), Explanations of Benefits (EOB) statements, and medical bills for suspicious charges.			
Total each column			

Grand Total _____

Scores:

0–6: You are not taking many actions to minimize your risk of identity theft. Consider what you have learned today, and see what steps you can take to protect your identity.

7–13: You have developed some good practices to avoid identity theft; however, you have room for improvement. Consider what actions you need to take or apply more regularly to better protect your identity.

14–20: You are doing a great job at minimizing your risk of identity theft. Continue to apply these actions regularly and determine what additional steps you can take to protect your identity

Planning For Unexpected Life Events

Planning ahead:

- Gives you control and options for your situation
- Relieves the stress of decision-making from caretakers/family members
- Saves money and helps you avoid financial disaster or setback
- Allows time for gathering information, comparing options, and determining which options help achieve what is most important

Preparing for possible future health problems

The majority of people who need long-term care are older adults. However, the need for long-term care can come at any age due to disabling diseases, car accidents, brain injuries, strokes, and other disabling events.

Families and individuals who plan ahead before a disability will be in a better position to cope in the event of a disability. Consider taking these steps before you or a family member becomes ill or disabled:

The need for long-term care can come at any age, plan ahead.

- **Prepare a plan.** Start with reviewing your income and expenses.
- **Make sure trusted family members know where to find personal and financial documents in an emergency.**
- **Set up direct deposit for income and benefit checks.** Direct deposit delivers your Social Security or Supplemental Security Income (SSI) benefit or other income sources into your bank, savings and loan, or credit union account quickly and safely.
- **Consider automatic payment** of important, recurring bills.
- **Consider a durable power of attorney.** As we mentioned in the section on power of attorney, this legal document gives one or more people the authority to handle finances and remains in effect if you become incapacitated.
- **Make sure you are properly insured.** Speak with a financial planner or an insurance agent you trust. Review your policy regularly because your needs can change.
- **Maintain a healthy lifestyle.**

Experts also recommend a health care power of attorney (also known as a health care proxy, advance directive or by another name, depending on the state) designating a family member or other trusted person to make decisions about medical treatment. Health care powers of attorney are intended to ensure that someone's wishes regarding medical care are honored.

Direct Deposit of your Social Security Benefit

Let's go into a little more detail about direct deposit of your Social Security and Supplemental Security Income (SSI) benefit payments. Applicants filing for these benefits must now choose either direct deposit or the Direct Express® debit card. Currently entitled beneficiaries and recipients who had been receiving payment by check generally had to switch to direct deposit to a checking account or a pre-paid card they select or to the Direct Express® debit card.

The U.S. Treasury sends an electronic message to your bank, savings and loan, or credit union crediting your account with the exact amount of your Social Security or SSI benefit. You can withdraw money, put some in savings or pay bills - the ordinary things you do with your money. The difference is, your check isn't printed or mailed. For more information, visit the Department of the Treasury's Go Direct® website **godirect.org**.

How to Be Financially Prepared for Disasters

Natural or man-made disasters can strike without warning and can happen anywhere. These include floods, fires, earthquakes, tornadoes, hurricanes, chemical spills or similar events that can force people to evacuate their homes. Even minor disasters can damage or destroy property or other belongings. They can also seriously impair your ability to conduct essential financial transactions for a period of time.

In addition to planning for your personal safety and basic needs (e.g., shelter, food, and water), you should be ready to deal with financial challenges, including how to pay for supplies or temporary housing if necessary.

What to Have Ready

Consider keeping the following documents, bank products, and other items in a secure place and readily available in case of an emergency:

- **Forms of identification:** These primarily include driver's licenses (or state identification cards for non-drivers), insurance cards, Social Security card, passport, and birth certificate.
- **Your checkbook with enough blank checks and deposit slips to last at least a month.**
- **ATM cards, debit cards (for use at ATMs and merchants), and credit cards:** Do not assume that merchants and ATMs in areas affected by a disaster will immediately be functioning as usual. Have other options available for getting cash and making payments.
- **Cash.**
- **Telephone numbers for your financial services providers:** These include local and toll- free numbers for your bank, credit card companies, brokerage firms (for stocks, bonds, or mutual fund investments) and insurance companies.
- **Important account numbers:** These include bank and brokerage account numbers, credit card numbers, and homeowner's or renter's insurance policy numbers. You may want to copy the front and back of your credit cards (and keep them in a safe place).
- **The key to your safe deposit box.**

What to Keep and Where to Keep It

After you have gathered your most important financial items and documents, protect them as well as you can while also ensuring you have access to them in an emergency. Here is a reasonable strategy for many people:

- Make backup copies of important documents.
- Make an electronic image of your documents so you can more easily store the information.
- Give a copy of your documents to loved ones or let them know where to find the documents in an emergency.
- Store your backups at some distance from your home in case the disaster impacts your entire community.
- Make a record of all credit/debit cards with the account and contact numbers to report lost/stolen cards.

Determine what to keep at home and what to store in a safe deposit box at your bank.

A safe deposit box is best for protecting items of value and certain papers that could be difficult or impossible to replace, but not anything you might need to access quickly.

Seal important documents in airtight and waterproof plastic bags or containers to prevent water damage.

What should you put in a safe deposit box? Examples include a birth certificate and originals of important contracts. What is better left safely at home, preferably in a durable, fireproof safe? Your passport and medical care directives, because you might need these on short notice. Consult your attorney before putting an original will in a safe deposit box. Some states do not permit immediate access to a safe deposit box after a person dies, so there may be complications accessing a will stored in a safe deposit box. Remember that safe deposit boxes are not necessarily fireproof or waterproof.

Prepare one or more emergency evacuation bags. Pack essential financial items and documents (e.g., cash, checks, copies of your credit cards and identification cards, a key to your safe deposit box, and contact information for your financial services providers). Make sure each evacuation bag is waterproof and easy to carry. Keep it in a secure place in your home. Periodically update the contents of the bag. It will not do you any good if the checks in your bag are for a closed account.

What Else to Consider

- **Arrange for automatic bill payments from your bank account.** This service enables you to make scheduled payments (e.g., for your telephone bill, insurance premiums and loan payments), and avoids late charges or service interruptions.
- **Sign up for Internet banking services.** This also makes it possible to conduct your banking business without writing checks. Only do this if you feel comfortable with keeping your internet security software up-to-date.
- **Review your insurance coverage.** Make sure you have enough insurance, including personal property coverage, as applicable, to cover the cost to replace or repair your home, car and other valuable property.

To learn more about being financially prepared for disasters, visit **fdic.gov/consumernews** and type "disaster" in the *Search FDIC Consumer News articles by topic* box.

ACTIVITY 4: How Financially Prepared Are You?

Reflect on what you have learned today. In the space provided, jot down what documents you will gather and where you will put them.

Scams that Target Homeowners

Reverse Mortgage Proceeds Fraud

Scenario
To pay for his recommended home improvements, a handyman convinces an older woman to appoint him as her agent under a power of attorney so he can help her get a reverse mortgage on the home she had purchased in the 1950s and owns outright. When the lender provided a lump-sum payout, she never saw any of the money because the handyman used it for drugs, among other things.

A reverse mortgage is a loan that allows homeowners age 62 and older to borrow against the equity in their homes.

What is a reverse mortgage?

Although reverse mortgages are legitimate products and are appropriate for some consumers, scammers also sell these products to the disadvantage of their victims.

A reverse mortgage is a special type of loan that allows homeowners age 62 and older to borrow against the equity in their homes. It is called a "reverse" mortgage because you receive money from the lender, instead of making payments as you would with a traditional mortgage. The money you receive, and the interest charged on the loan, increases the balance of your loan each month. Over time, the equity you have in your home decreases as the amount you owe increases.

When you take out a reverse mortgage loan, you can receive your money as a line of credit available when you need it, in regular monthly installments, or up-front as a lump sum. You do not have to pay back the loan as long as you continue to live in the home, maintain your home, stay current on expenses such as homeowner's insurance and property taxes. If you move out or die, or fall behind on property taxes or homeowner's insurance, the loan becomes due and must be paid off.

For more information go to **ASK CFPB consumerfinance.gov/askcfpb/reversemortgage** and consult the CFPB consumer guide *Considering a Reverse Mortgage* **consumerfinance.gov/f/201206_cfpb_Reverse_Mortgage_Guidance.pdf** to help you ask the right questions before applying for a reverse mortgage.

How Borrowers Get Scammed

Scammers can take advantage of the fact that borrowers can receive the loan in the form of a lump sum payout. The reverse mortgage proceeds scam may include one or several of the following elements:

- Family members or others who pressure the older adult to get a reverse mortgage and then "borrow" the money or scam the elder out of the proceeds.
- Scammers who "require" an older borrower to sign a power of attorney or to sign proceeds over to a "loan officer or other agent" for future "disbursals." The scammers then embezzle a portion or all of the funds.
- Brokers who pressure or fraudulently require the borrower to purchase annuities, long- term care insurance, high risk investments or other financial products with the proceeds from the reverse mortgage in order to generate additional commissions.

Mortgage Assistance Rescue Scam

Beware of anyone who promises you can stay in your home or who asks for a lot of money to help you. Scammers might promise guaranteed or immediate relief from foreclosure, and they might charge you very high fees for little or no services.

Foreclosure prevention counseling is available free of charge through HUD's Housing Counseling Program.

Mortgage relief companies may not collect any fees until they have provided you with a written offer from a lender or servicer that you decide is acceptable and a written document from the lender or servicer describing the key changes to the mortgage that would result if you accept the offer. The companies also must remind you of your right to reject the offer without any charge.

Don't get scammed. There is help available at little or no cost to you. Foreclosure prevention counseling is available free of charge through HUD's Housing Counseling Program. Visit HUD's website (go.usa.gov/v2H) or call 1-800-569-4287) to find a qualified reverse mortgage counselor near you.

Contractor Fraud and Home Improvement Scams

Sooner or later every home needs repairs or improvements. Although some home improvement companies do good work, some may not provide the level of service you expect. Many homeowners are targeted by scam artists who use high pressure tactics to sell unneeded and overpriced contracts for "home improvements." Often these scam artists charge more than their quoted prices or their work does not live up to their promises. When the homeowner refuses to pay for shoddy or incomplete work, the contractor or an affiliated lender threatens foreclosure on the home. Con artists may pose as building inspectors and order immediate repairs which they can do on the side. They may also pose as government officials and demand a fee for processing emergency loan documents.

Home Improvement Scam Scenario

Monica is 76 years old and lives alone in her home. One morning she is outside watering her garden when a truck pulls up and a man approaches her. He tells her that he is a building contractor and that he can see that she has a problem with her roof. He points to a spot near the chimney and tells her he can fix the problem now with the materials he has left over from a job he just finished nearby. He says he'll give her a big discount if she'll pay him today in cash. After going up on the roof and tearing off some roof tiles, he tells her that the problem is worse than he thought, but he can do it for $2,800. When Monica says she doesn't have $2,800 in cash, the contractor becomes angry and threatening. He says if Monica doesn't have the money she will have to take out a loan to pay him.

Tips for Avoiding Contractor Fraud

Here are some common sense tips to protect yourself from contractor fraud.

- Ask to see identification for anyone representing him or herself as a government official.
- Call the government agency to verify the identity if there is any payment of money involved.
- Get bids from several local, established contractors. Obtain at least three legible bids in writing. Don't sign anything before carefully reading it. Do not do business with anyone who approaches you door-to-door or on the phone. Note that many states and local jurisdictions have laws regulating door-to-door sales.
- Avoid contractors who
  - Are working door-to-door
  - Come from out of state
  - Don't provide an address and telephone number, or refuse to show identification

Don't pay in advance.

- Before beginning any home repair project, ask if the contractor has the required licenses (note license numbers) and is bonded. Seek out references from neighbors or members of your affinity groups (e.g., place of worship).
- Check with your state licensing agency's website or hotline to make sure the licenses are valid. Ask the licensing agencies if the contractor has a history of complaints.
- Get several references from previous customers. If possible, visit them to see the work done.
- Require the contractor you choose to provide you with a contract that contains clearly written payment terms.

- Don't pay in advance.
- Never pay with cash.
- Don't provide personal financial information, such as your checking account, credit card or debit card numbers.
- If you need to borrow money to pay for repairs, don't let the contractor steer you toward a particular lender.
- Do not make a final payment until you are satisfied with the job, all debris is removed from your property, and any necessary building inspections have been completed.
- If a contractor shows up at your door and pressures you to go to the bank with him to get cash to pay for a job you do not want done, ask to speak with the branch manager. The manager can call the police for you, who can show up at the branch. Being in a public place with video cameras and witnesses should reduce your risk.

To get more information on home improvement, including how to hire contractors, how to understand your payment options, and how to protect against home improvement scams, read the FTC brochure titled Hiring a Contractor. The brochure is available at **consumer.ftc.gov/articles/how-avoid-home-improvement-scam**. You can also call the FTC to request the brochure at 1-877-FTC-HELP (382-4357).

Scams that Target Veterans

Pension Benefits Filing Scam

The Veterans Benefits Administration provides monthly benefit payments to certain wartime veterans with financial need, and their survivors. Recipients also may be eligible for one of two additional amounts:

- Aid and Attendance (A&A) may be paid to veterans, or their surviving spouses, who require assistance with activities of daily living, are bedridden, are patients in nursing homes, or have a qualifying major vision loss.
- Housebound benefits may be paid to veterans or surviving spouses who are substantially confined to their homes because of a permanent disability.

Unfortunately, some individuals scam veterans or their surviving spouses by charging them fees to prepare or file a claim.

Tips for avoiding VA pension benefits filing scams

- Be aware that an individual generally must be accredited by VA to assist you in preparing and filing a claim. To find an accredited attorney, claims agent, or veterans service organization (VSO), visit VA's Accreditation Search page at **va.gov/ogc/apps/accreditation/index.asp**
- Never pay a fee to anyone for preparing and filing your initial claim.
- Although an attorney may charge a consulting fee for advising you about the benefits for which you may be eligible, the clock stops running as soon as you indicate your intention to file.

- Avoid attorneys or claims agents who try to market financial products, such as trusts and annuities, in connection with filing your VA claim. Older veterans may face problems with annuities since you may not have access to your funds, should you need them, without paying a costly surrender fee.
- Know that shifting your assets into certain types of investments in order to meet eligibility thresholds for VA pension benefits could make you ineligible for Medicaid for a period of time.

Pension Advance Scam

Another scam targets older adults who receive either monthly disability compensation or pension payments. The scammer may offer a cash advance on monthly pension payments. These scams are also called "lump sum buyouts." Whatever the name, these transactions generally are not a good deal for the veteran or other retired government workers who are frequently targeted.

Consider this example:
A veteran received a cash advance of $73,000 in exchange for his monthly pension payment of $2,744 for a ten-year period. At the end of the ten years, the veteran's total repayment is estimated as $256,293. This translates to an annual interest rate of 44.5 percent.

Tips for avoiding the pension advance payment scam

Know that pension advance payment arrangements are very costly loans, and fees can sometimes be hidden.

Say no to arrangements that allow a creditor to access the account where you receive your benefits. This includes joint checking accounts shared with the company that allow the pension advance lender to take monthly withdrawals to pay for interest and other fees.

Remember that your military benefits cannot be garnished by a lender.

Remember that your military benefits cannot be garnished by a lender. Some pension advance lenders know this, so they may require you to take out a life insurance policy with the company as beneficiary.

If you're facing a financial emergency, professional financial coaches are available. Some non-profit credit counseling agencies charge sliding-scale fees so that consumers can afford their help. A professional can help you plan for future financial needs and goals.

Three ways you can protect your retirement pension:

- Avoid loans with high fees and interest. Pension advance companies may not always advertise their fees and interest rates, but you will certainly feel them in your bottom line. Before you sign anything, learn what you are getting and how much you are giving up.
- Don't sign over control of your benefits. Companies sometimes arrange for monthly payments to be automatically deposited in a newly created bank account so the company can withdraw payments, fees and interest charges from the account. This leaves you with little control.

- Don't buy life insurance that you don't want or need. Pension advance companies sometimes require consumers to sign up for life insurance with the company as the consumer's beneficiary. If you sign up for life insurance with the pension advance company as your beneficiary, you could end up footing the bill, whether you know it or not.

Where to Get More Information or Assistance

For more information review the CFPB's consumer advisories Protect Your Retirement Pension **go.usa.gov/x9H2c** and 3 Pension Advance Traps to Avoid **go.usa.gov/x9H2T**. The U.S. Administration on Community Living's Pension Counseling and Information Program currently serves 30 states and provides free legal assistance to individuals who are facing a problem with their pensions. For more information, visit **pensionhelp.org** or call 1-888-420-6550.

For help understanding VA benefits, visit **va.gov** or call 1-800-827-1000. Also, visit the Federal Trade Commission at **consumer.ftc.gov/articles/0349-veterans-pensions**.

Post-Test

Now that you have gone through the course, see what you have learned.

1. Who of the following may be perpetrators of elder financial exploitation? Select all that apply.
   - **a.** Family members and caregivers
   - **b.** Friends or neighbors
   - **c.** Telephone and mail scammers
   - **d.** Financial advisers

2. What is true of a durable power of attorney (POA)? Select all that apply.
   - **a.** It remains in place if you become incapacitated.
   - **b.** It allows the person you select to make financial decisions on your behalf.
   - **c.** It can be changed or revoked.
   - **d.** No one else can monitor the actions of your designated POA.

3. If you receive a call or an email from someone claiming to be in trouble and in need of emergency funds, what should you do? Select all that apply.
   - **a.** Call the individual at a known home or cell phone number to verify that the need is legitimate.
   - **b.** Immediately wire funds to the account number provided.
   - **c.** If the call is from a hospital or law enforcement agency, look up the number of the institution and call the number you find.
   - **d.** Hang up immediately.

4. Your bank will never send you an email asking you to verify your account number or any other identifying information.
   - **a.** True
   - **b.** False

5. Where can you check a financial adviser's background?

- **a.** FINRA BrokerCheck
- **b.** Social Security Administration
- **c.** State Securities Regulator
- **d.** Federal Trade Commission

6. Which forms of identification should you have readily available in case of emergency?

- **a.** Driver's License
- **b.** Insurance Card
- **c.** Social Security Card
- **d.** Passport
- **e.** Birth Certificate

7. What can you do to prepare financially for a disaster?

- **a.** Set up automatic bill payments.
- **b.** Know where to find important documentation in an emergency.
- **c.** Review insurance information regularly to ensure you have adequate coverage.
- **d.** All of the above.

8. What practices should you avoid in selecting someone to repair your roof?

- **a.** Getting three bids in writing from local established contractors.
- **b.** Using contractors who come to your door and tell you they are working for a neighbor.
- **c.** Asking if the contractor has the required licenses and getting his/her license numbers.
- **d.** Paying in advance

9. Match these items with the best place to keep them:

Item	**Best place to keep**
1. Birth certificate	A. Emergency evacuation bag
2. Medical care directives	B. Safe-deposit box
3. Passport	C. Safe-deposit box
4. Important contracts	D. Fireproof safe
5. Items you may need in an emergency	E. Fireproof safe

What Do You Know? – Money Smart for Older Adults

Instructor:_____

Date:_____

This form will allow you and the instructors to see what you know about protecting your finances both before and after the training. Read each statement below. Please circle the number that shows how much you agree with each statement.

Before the Training I am able to:	**Strongly Disagree**	**Disagree**	**Agree**	**Strongly Agree**
1. Recognize elder financial exploitation.	1	2	3	4
2. Guard against identity theft.	1	2	3	4
3. Plan for unexpected loss of the ability to manage my finances.	1	2	3	4
4. Prepare financially for disasters.	1	2	3	4
5. Find other helpful resources for managing my money.	1	2	3	4

After the Training I am able to:	**Strongly Disagree**	**Disagree**	**Agree**	**Strongly Agree**
6. Recognize elder financial exploitation.	1	2	3	4
7. Guard against identity theft.	1	2	3	4
8. Plan for unexpected loss of the ability to manage my finances.	1	2	3	4
9. Prepare financially for disasters.	1	2	3	4
10. Find other helpful resources for managing my money.	1	2	3	4

OMB No. 3170-0024 (Expiration Date: 11/30/2018)

Evaluation Form

This evaluation will enable you to assess your observations of the Money Smart for Older Adults module. Please indicate the degree to which you agree with each statement by circling the appropriate number.

Overall, I felt the module was:	**[ ] Excellent** **[ ] Very Good** **[ ] Good** **[ ] Fair** **[ ] Poor**

	Strongly Disagree	Disagree	Agree	Strongly Agree
1. I achieved the training objectives.	1	2	3	4
2. The instructions were clear and easy to follow.	1	2	3	4
3. The slides were clear.	1	2	3	4
4. The slides enhanced my learning.	1	2	3	4
5. The time allocation was correct for this module.	1	2	3	4
6. The module included sufficient examples and exercises so that I will be able to apply these new skills.	1	2	3	4
7. The instructor was knowledgeable and well-prepared.	1	2	3	4
8. The worksheets are valuable.	1	2	3	4
9. I will use the worksheets again.	1	2	3	4
10. The participants had ample opportunity to exchange experiences and ideas.	1	2	3	4
11. I had knowledge of the subject matter before taking the module.	1	2	3	4
12. I have knowledge of the subject matter upon completion of the module.	1	2	3	4

OMB No. 3170-0024 (Expiration Date: 11/30/2018)

13. Name of Instructor:

Please use the response scale and circle the appropriate number.	Strongly Disagree	Disagree	Agree	Strongly Agree
Objectives were clear & attainable	1	2	3	4
Made the subject understandable	1	2	3	4
Encouraged questions	1	2	3	4
Had technical knowledge	1	2	3	4

What was the most useful part of the training?

What was the least useful part of the training and how could it be improved?

Privacy Act Statement
5 U.S.C. 552(a)(e)(3)
The information you provide to the Bureau of Consumer Financial Protection ("BCFP"), will only be used to evaluate the Money Smart for Older Americans Training Sessions. Information collected will be treated in accordance with the System of Records Notice ("SORN"), CFPB.021 – CFPB Consumer Education and Engagement Records, 77 F.R. 60382. This information will only be disclosed as outlined in the Routine Uses for the SORN. Direct identifying information will only be used to facilitate the evaluation of the training and will be kept private except as required by law. This collection of information is authorized by Pub. L. No. 111-203, Title X, Sections 1013 and 1022, codified at 12 U.S.C. §§ 5493 and 5512. Participation in this evaluation is voluntary, you are not required to participate or share any identifying information and you may withdraw participation at any time. However, if you do not include the requested information, you may not be able to participate in the evaluation.

Paperwork Reduction Act
According to the Paperwork Reduction Act of 1995, an agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a valid OMB control number. The OMB control number for this collection is 3170-0024. The time required to complete this information collection is estimated to average approximately 5 minutes per response. Comments regarding this collection of information, including the estimated response time, suggestions for improving the usefulness of the information, or suggestions for reducing the burden to respond to this collection should be submitted to Bureau at the Bureau of Consumer Financial Protection (Attention: PRA Office), 1700 G Street NW, Washington, DC 20552, or by email to PRA@cfpb.gov.

OMB No. 3170-0024 (Expiration Date: 11/30/2018)

Glossary

Adult Protective Services (APS): A state or local agency that investigates abuse, neglect or exploitation of older persons or adults who have disabilities.

Affinity Fraud: A type of fraud that targets members of an identifiable group, such as a religious organization, ethnic group, older adults, or professional groups.

Agent: A person to whom you grant authority to act in your place.

Annuity: A type of investment offered by insurance companies, or by other financial institutions acting on behalf of insurance companies. Annuities allow your money to grow tax-deferred until you withdraw it. The insurer agrees to make periodic payments to you for a set period of time. Annuities are complex investments with a variety of structures. They are not appropriate for many people in or near retirement.

Variable Annuity: An insurance contract that invests your premium in various mutual fund-like investments.

Direct Deposit: An electronic method for transferring and depositing money directly into your account.

Direct Express Debit Card: A debit card that allows you to access your federal benefits without a bank account. Your federal benefits payment is deposited to your Direct Express® card account on your payment day. You can use the card to make purchases, pay bills or get cash.

Elder Financial Exploitation: The Older Americans Act defines elder financial exploitation quite broadly, as "the fraudulent or otherwise illegal, unauthorized, or improper act or process of an individual, including a caregiver or fiduciary, that uses the resources of an older individual for monetary or personal benefit, profit, or gain, or that results in depriving an older individual of rightful access to, or use of, benefits, resources, belongings, or assets."

Electronic Transfer Account (ETA): A low-cost account that allows recipients to receive their federal payments electronically.

Fiduciary: Someone named to manage money or property for someone else. Fiduciaries must act in the other person's best interest and follow four basic duties:

1. Act only in the older person's best interest
2. Manage the older person's money and property carefully
3. Keep the older person's money and property separate from theirs
4. Keep good records

Federal Deposit Insurance Corporation (FDIC) Deposit Insurance: Insurance that protects your money if the bank fails. However, FDIC does not insure non-deposit investment products, including stocks, bonds, mutual funds, and annuities.

Fraud: A type of illegal act involving the obtaining of something of value through willful misrepresentation.

Grandparent Scam: A scam whereby a caller pretends to be a relative in need of immediate funds to deal with an emergency. The caller may also represent themselves as a hospital employee, law enforcement officer, or attorney.

Identity Theft: A fraud committed or attempted using the identifying information of another person without authority.

Older Adult: Someone age 62 or older.

Older Americans Act: Legislation initially passed in 1965, which established authority for grants to States for community planning and social services, research and development projects, and personnel training in the field of aging. It established the Administration on Aging (AoA) to administer the newly created grant programs. Today, it is called the Administration for Community Living (ACL) and it authorizes a wide array of service programs through a national network of state agencies on aging, area agencies on aging, service providers, Tribal organizations, and native Hawaiian organizations.

Pharming: When criminals seek to obtain personal or private information by making fake websites appear legitimate.

Phishing: When criminals send out unsolicited emails that appear to be from a legitimate source in an attempt to trick you into divulging personal information.

Ponzi Scheme: Also called a "pyramid" scheme. The scam artists promise high returns and use the money of later investors to pay off other earlier investors.

Power of Attorney: A legal document that allows someone to manage your property or belongings.

Durable Power of Attorney: A power of attorney (POA) that remains in effect even if you become incapacitated.

Privacy Notices: Notices that explain how the company handles and shares your personal financial information. You will usually receive a privacy notice when you open an account or become a customer of a financial company, once a year after opening an account, and any time the financial company changes its privacy policy.

Promissory Note: A form of debt – similar to a loan or an IOU – that a company may issue to raise money.

Reverse Mortgage: A special type of loan that allows homeowners age 62 and older to borrow against the equity in their homes.

Revocable Trust Account: A deposit account owned by one or more people that designates one or more beneficiaries who will receive the deposits upon the death of the owner(s).

Romance scam: A romance scam is when a new love interest says they love you, but they just want your money—and they may not be who they say they are. Romance scams can happen online or in person.

Scam: A confidence trick, confidence game, or con for short; an attempt to intentionally mislead a person or persons usually with the goal of financial or other gain.

Spam: Unsolicited commercial email (UCE).

Spoofing: Deception or hoax.

Surrender Charge: A fee you incur when you sell, or cancel, certain types of investments or annuity policies.

For Further Information

Consumer Financial Protection Bureau (CFPB)
consumerfinance.gov
1-855-411-2372

The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act) created the Consumer Financial Protection Bureau to make markets for consumer financial products and services work for Americans. The Bureau works to fulfill this mission by making rules more effective, by consistently and fairly enforcing those rules, and by empowering consumers to take more control over their economic lives.

The Office for Older Americans is a special office within the CFPB's Division of Consumer Education and Engagement dedicated to helping Americans age 62 and older make sound financial decisions.

The CFPB offers several resources:

- Print brochures such as Considering a Reverse Mortgage, Know Your Financial Adviser and the Managing Someone Else's Money guides can be found by visiting **consumerfinance.gov/older-americans**.
- An online resource called ASK CFPB, which contains authoritative, unbiased, understandable answers to commonly-asked consumer questions with a special section for older Americans, at **consumerfinance.gov/askcfpb**.
- An online tool called Planning for Retirement to help you make an informed decision about when to claim your Social Security retirement benefits. The tool is available at **consumerfinance.gov/retirement**.
- Handling of consumer complaints about financial products and services including mortgages, money transfers, debt collection, credit cards, prepaid cards, bank accounts and services, vehicle and other consumer loans, payday loans, student loans, credit reporting, and virtual currency. Complaints can be submitted online at **consumerfinance.gov/complaint** or by calling 1-855-411-2372.

Federal Deposit Insurance Corporation (FDIC)
fdic.gov/education
Division of Depositor & Consumer Protection
2345 Grand Boulevard, Suite 1200
Kansas City, Missouri 64108
1-877-ASK-FDIC (275-3342)

Visit the FDIC's website for additional information and resources. Additional Money Smart financial education program resources are available for all ages and in different formats, including online as computer based instruction. And, the quarterly FDIC Consumer News provides practical hints and guidance on how to become a smarter, safer user of financial services. Also, the FDIC's Consumer Response Center is responsible for:

- Investigating all types of consumer complaints about FDIC-supervised institutions
- Responding to consumer inquiries about consumer laws and regulations and banking practices

Consumers should note that while the FDIC is responsible for insuring deposits in FDIC insured institutions, the bank itself may be chartered or supervised by other agencies (such as the Office of the Comptroller of the Currency or the Federal Reserve). To determine which regulator has jurisdiction over a particular banking institution, so you can submit a complaint to the correct agency, you can call the FDIC toll-free at 1-877-ASK-FDIC 1-877-275-3342. For consumer protection issues, you can also contact the CFPB.

Federal Trade Commission (FTC)
ftc.gov
1-877-FTC-HELP (382-4357)
ftc.gov/idtheft
1-877-IDTHEFT (438-4338)

The Federal Trade Commission FTC website offers practical information on a variety of consumer topics. The **Identitytheft.gov** website offers information on what to do if you are the victim of identity theft.

"Pass It On," the Federal Trade Commission's newest education effort, is aimed at active older adults, ages 65 and older—a huge group with life experience and a social network. "Pass It On" sees older adults as part of the solution, not simply victims of the actions of others, and gives them articles, presentations, bookmarks, activities, and a video – everything they need to start a conversation about scams and pass on what they know. For more information visit **ftc.gov/passiton**.

Eldercare Locator
eldercare.acl.gov
1-800-677-1116

The Eldercare Locator, a public service of the Administration for Community Living, U.S. Department of Health and Human Services, is a nationwide service that connects older adults and their caregivers with information on senior services in their state. You can search for services by location or by topic.

Medicare
medicare.gov
1-800-MEDICARE (1-800-633-4227)

The official U.S. Government site for Medicare allows you to search for physicians and other health care providers that are enrolled in Medicare.

U.S. Department of Veterans Affairs
va.gov
1-800-827-1000

To find a list of accredited representatives, agents, and attorneys who can assist you in filing for benefits, visit **va.gov/ogc/apps/accreditation/index.asp**.

National Center on Elder Abuse
ncea.acl.gov/

The Administration for Community Living sponsored website provides resources on elder abuse prevention, including information on reporting a suspected case of elder abuse.

Financial Industry Regulatory Authority
finra.org
1-800-289-9999 (BrokerCheck Hotline)
Find out about the broker's background via the **brokercheck.finra.org**. Or call the FINRA BrokerCheck Hotline. Find out more about the use of senior designations or certifications at **finra.org/investors**

OnGuardOnline.gov
onguardonline.gov

OnGuardOnline.gov is the federal government's website to help you be safe, secure and responsible online. The FTC manages the site in partnership with 16 other federal agencies. Its resources include information on phishing available at **onguardonline.gov/articles/0003-phishing**.

Financial Fraud Enforcement Task Force (FFETF)
stopfraud.gov/protect-yourself.html

This is a task force composed of government agencies that has a website with resources on Elder Fraud.

Report Financial Exploitation

If someone is in immediate danger, dial 911 or your local police department.

Adult Protective Services
Telephone numbers vary by location
Visit **eldercare.acl.gov** or
call for contact information for your area: 1-800-677-1116
APS is a state or local government agency, generally a part of your county or state department of social services, that investigates abuse, neglect or exploitation of older adults, or younger adults who have disabilities.

Federal Trade Commission (FTC)
consumer.ftc.gov

Call 1-877-IDTHEFT (438-4338) or visit **ftc.gov/idtheft**
The FTC online toolkit includes a detailed guide for protecting your information, with instructions and sample letters to help identity theft victims – Taking Charge: What to Do If Your Identity Is Stolen. An online complaint form is available directly at **ftccomplaintassistant.gov**.

Legal advice or representation.

How can I find an attorney who specializes in elder law issues?

Federally funded legal assistance programs for people 60 and older (known as Title IIIB legal services programs) can provide legal assistance on issues such as income security, health care, long-term care, nutrition, housing, utilities, protective services, defense of guardianship, abuse, neglect, and age discrimination. Legal assistance is targeted towards older individuals in social and economic need. Each program has its own priorities and eligibility guidelines regarding case acceptance and areas of representation. Your senior legal aid program may be located at your local legal services program. You can also find out about your local legal assistance programs by contacting your area agency on aging or **eldercare.acl.gov**. If you need a private attorney to assist you with making a power of attorney, trust, will or other advance planning tool, contact your state bar association to find a lawyer referral service.

Senior Medicare Patrol (SMP)
smpresource.org
1-877-808-2468

The SMP, also known as Senior Medicare Patrol, helps Medicare and Medicaid beneficiaries avoid, prevent, and detect health care fraud. SMPs nationwide recruit and teach nearly 5,700 volunteers every year to help in this effort. Most SMP volunteers are both retired and Medicare beneficiaries and thus well-positioned to assist Medicare beneficiaries and others. Visit the website above or call for more information or to get contact information for your state SMP.

Social Security Administration (SSA)
ssa.gov
Toll free customer service at 1-800-772-1213.
Individuals who are deaf or hearing-impaired can call Social Security's TTY number at 1-800-325-0778.

***my* Social Security** is a free online account that allows people quick, secure access to their personal Social Security information. Establishing this account protects you and keeps your personal Social Security information private. Individuals can use ***my* Social Security** to access their Social Security Statement to check their earnings and get estimates of future retirement, disability, and survivor benefits you and your family may receive.

If you already receive Social Security benefits, you also can get your benefit verification letter, change your address and phone number, and start or change direct deposit information. You also can get a replacement form SSA-1099/SSA-1042S (which is used when filing taxes) and shows you how much you received in Social Security benefits in the past year. To create an account, visit **socialsecurity.gov/myaccount** and select "Create An Account." You will have to provide some personal information about yourself and give them answers to some questions only you are likely to know to verify your identity. Next, you choose a "username" (8 to 20 letters and/or numbers) and an "8-character password" (at least one capital letter, one lowercase letter, at least one number and at least one symbol) to access your online account.