MONEY SMART

for Older Adults

cfpb Consumer Financial Protection Bureau

FDIC FEDERAL DEPOSIT INSURANCE CORPORATION

OBJECTIVES

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

WHAT DO YOU KNOW?

What is elder financial exploitation and who is at risk?

WHAT IS ELDER FINANCIAL EXPLOITATION?

- Fraudulent or otherwise illegal, unauthorized, or improper act or process of an individual that uses the resources of an older person for personal benefit, profit or gain
- Actions that result in depriving an older person of rightful access to, or use of benefits, resources, belongings, or assets

WHO IS AT RISK?

Anyone can be the victim of financial exploitation.

Elder financial exploitation crosses all social, educational, and economic boundaries.

WHY ARE OLDER ADULTS AT RISK?

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 a loss
- 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

WHY ARE OLDER ADULTS AT RISK? (cont.)

Some older adults may:

- Be receiving care from a person with financial or other 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 or another person who may pressure them for money

EXAMPLES OF FINANCIAL EXPLOITATION

Exploitation by an agent under a POA or person in another fiduciary relationship

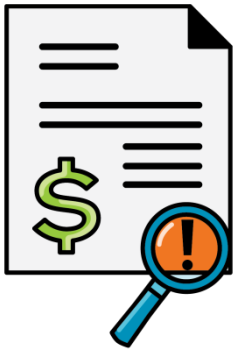
Investment fraud and scams

Theft of money or property by family members, caregivers, or in-home helpers

Lottery and sweepstakes scams

EXAMPLES OF FINANCIAL EXPLOITATION (cont.)

Grandparent/ Imposter scams



Tax and debt collection scams

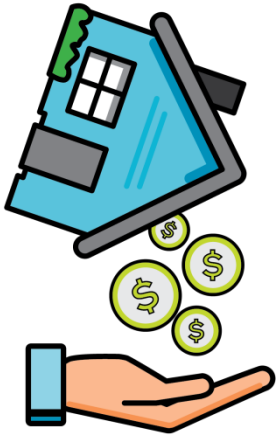
Charity scams

Telemarketer, mail offer or salesperson scams

EXAMPLES OF FINANCIAL EXPLOITATION (cont.)

Telephone, computer, and internet scams

Identify theft



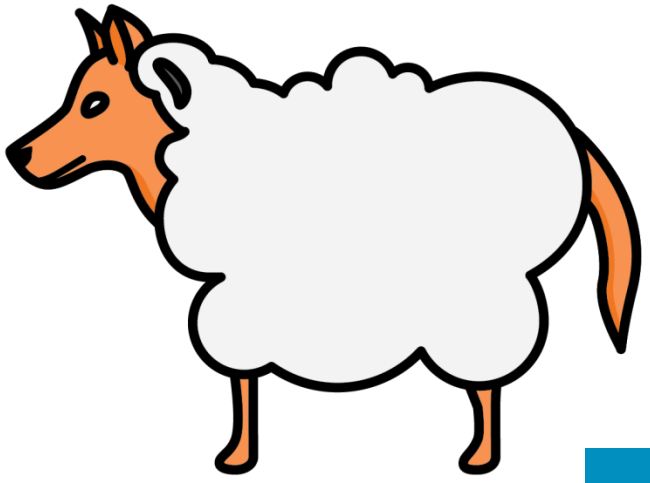
Reverse mortgage fraud

Contractor fraud and home improvement scams

WHO ARE THE ABUSERS?

People you know

- Family members and caregivers
- Friends, neighbors or acquaintances
- Agents under a power of attorney
- Financial advisers



WHO ARE THE ABUSERS?

Strangers

- Telephone and mail scammers
- Internet scammers
- Home repair contractors
- Medicare scam operators
- Others

WHY DON’T OLDER ADULTS REPORT EXPLOITATION?

- Shame and embarrassment
- Loyalty to a family member or caregiver
- Fear of retaliation or not being believed
- Dependence on the abuser
- Denial
- Self-blame
- Lack of awareness

WHO CAN HELP?

Adult Protective Services

For elder abuse, contact Adult Protective Services.

Find contact information eldercare.gov or

call 1-800-677-1116.

Local Police - 911

If someone is in danger or a crime has been committed, call the police.

WHO CAN HELP? (CONT.)

For concerns about a financial institution

For example:

- Bank
- Credit Union

contact the financial institution

For concerns about credit products

contact the creditor

You are often not responsible for unauthorized credit card charges or payments.

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

EXPLOITATION BY A FIDUCIARY

Fiduciary

a person who is named to manage your money or property

Fiduciary Duties

1. Acts only in your interest
2. Manages your money and property carefully
3. Keeps your money and property separate from his/hers
4. Keeps good records

WHAT IS A POWER OF ATTORNEY?

POA

a legal document that allows someone else to handle your finances on your behalf

- Appoints a substitute decision-maker who can handle finances on your behalf
- Generally, avoids the need for a court-appointed guardian
- Is relatively inexpensive to create; advisable to use a lawyer

POWER OF ATTORNEY: RISKS

- **Pressure to grant more authority than you wish**
- **Misuse of your funds**
- **Unauthorized actions**
  (e.g., make gifts if you didn’t grant that power)

POWER OF ATTORNEY

- A durable POA remains effective even if the grantor loses the capacity to make financial decisions
- An attorney can help make an appropriate POA for your circumstances

POWER OF ATTORNEY: SAFEGUARDS

- Trust but verify
- Avoid appointing anyone who mismanages money or has personal issues.
- Tell trusted professionals about your POA, including your financial institution so they can look out for misuse
- If needed, change, cancel, or revoke the POA
- Avoid appointing hired caregivers/helpers
- Beware of new “best friends” who offer to handle your finances

TIP: 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.

HELP YOUR FIDUCIARY HELP YOU

The CFPB's plain language guides help fiduciaries:

- Walk them through their duties
- Tell them how to watch out for scams and financial exploitation, and what to do if their loved one is a victim
- Tell them where to go for help

consumerfinance.gov/managing-someone-elses-money

IF YOU ARE A VICTIM

Report financial exploitation immediately to Adult Protective Services or your local law enforcement agency.

ABUSE BY CAREGIVERS AND IN-HOME HELPERS

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

CAREGIVER: SAFEGUARDS

- Secure private financial documents
- Require receipts for purchases made
- Monitor bank accounts and telephone bills
- Consider setting up:
  - Automatic bill pay systems
  - Transaction alerts

CAREGIVER: SAFEGUARDS (cont.)

- Do not let hired caregivers open your mail, pay your bills, manage your finances
- Never promise money or assets after you die in exchange for care now
- Never lend employees money or property
- Never let caregivers use your credit or ATM card

CAREGIVER: SAFEGUARDS (cont.)

- Have someone else read your financial statements, if you are having trouble reading
- Secure your valuables
- Check your free credit reports at annualcreditreport.com

INVESTMENT FRAUD

- Misleading senior certifications/designations
- Ponzi schemes
- Unscrupulous financial advisers
- Affinity fraud
- Internet fraud – the “Dot-Con”
- Inappropriate or fraudulent annuities

INVESTMENTS: SAFEGUARDS

- Check the background of a broker or brokerage firm, or an investment adviser at brokercheck.finra.org or 1-800-289-9999

- Check the background of a Registered Investment Adviser at adviserinfo.sec.gov

INVESTMENTS: SAFEGUARDS (cont.)

- The North American Securities Administrators Association (NASAA) provides information for contacting state regulators nasaa.org/about-us/contact-us/contact-your-regulator/
- Consult CFPB consumer guide *Know Your Financial Adviser* at consumerfinance.gov/blog/know-your-financial-adviser

INVESTMENTS: SAFEGUARDS (cont.)

- Don’t trust strangers, no matter how trustworthy they sound
- Take time to understand your investment choices
- Say “no” to pressure
- Be wary of salespeople who prey on fears or promise returns that seem “*too good to be true*”

INVESTMENTS: SAFEGUARDS (cont.)

- Ask for a written explanation of every investment opportunity and get a second opinion
- Be wary of financial advisers who tell you to leave everything in their care
- Stay in charge of your money or enlist a trusted and capable third party

INVESTMENT: SAFEGUARDS (cont.)

- Make checks payable to a company or financial institution, never an individual
- Retain and maintain account statements and confirmations
- Document every conversation
- Don’t put all of your eggs in one basket

INVESTMENTS: IF PROBLEMS OCCUR

- Take immediate action if you detect a problem
- Don’t let embarrassment or fear stop you from reporting exploitation or fraud

TIMING IS CRITICAL.

INVESTMENTS: POINTERS

- Save enough to cover six months of living expenses before you invest
- Don’t make any investments unless you understand them fully
- Become better informed
- Be wary of marketing tactics like a free lunch seminar
- Understand the risk before investing
- Tell your financial adviser of your financial objectives and risk tolerance

UNDERSTANDING FDIC INSURANCE

What It Covers

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

What It Does Not Cover

- Stocks or Bonds
- Mutual Fund Shares
- Life Insurance Policies
- Annuities
- Municipal Securities
- Safe deposit boxes
- Losses resulting from theft, fraud or robbery

UNDERSTANDING FDIC INSURANCE (cont.)

- **Coverage – generally $250,000 per person per category**
- **Categories**
  - Single accounts
  - Joint accounts
  - Revocable trust accounts
  - Certain retirement accounts

For more information:

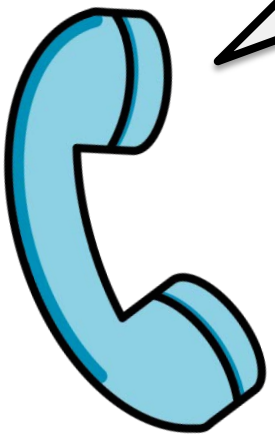
- **Contact FDIC: fdic.gov/deposit/deposits or call 1-877-ASK-FDIC**
- **Talk to your banker**

AVOID TELEPHONE AND INTERNET SCAMS

Scam artists on the telephone use lies, deception, and fear tactics

GRANDPARENT SCAM

Hello, Grandpa. I'm in trouble. Please don't tell Mom.



Scammers:

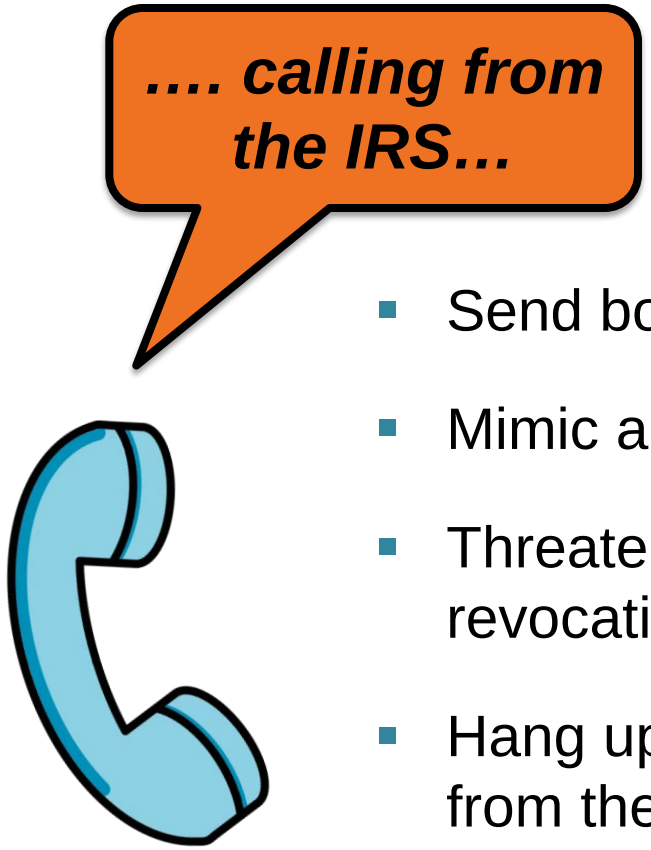
- May know grandchild's name
- Usually cry to disguise voice
- Plead for victim to wire money
- Ask not to tell family members

IRS TELEPHONE SCAM

Scammers:

- Say money is owed for taxes
- May use spoof (i.e., falsely represent) IRS toll-free numbers
- Use common names and fake IRS badge numbers
- May know the last 4 digits of a victim's Social Security number

IRS TELEPHONE SCAM (cont.)



- Send bogus IRS emails
- 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 Department of Motor Vehicles

IRS TELEPHONE SCAM (cont.)

The IRS always sends a written notification by the U.S. mail

The IRS never asks for payment or credit card information over the phone

The IRS never requests personal or financial information via email

WHAT TO DO

- If you owe taxes, call the IRS at 1-800-829-1040
- If you **don't** owe taxes:
  - Report the incident to the Treasury Inspector General for Tax Administration at: 1-800-366-4484 or www.tigta.gov
  - File a complaint via ftccomplaintassistant.gov

LOTTERY AND SWEEPSTAKES SCAMS

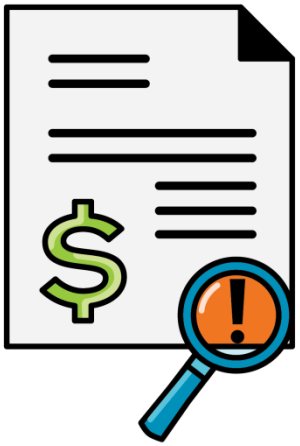
Scammers may:

- Call, email, or text regarding lotteries, drawings, or sweepstakes
- Request upfront processing fees or taxes
- Send authentic-looking claims checks
- Pose as an attorney for winners

TIPS FOR AVOIDING TELEPHONE SCAMS

- Cannot usually win a contest unless you enter
- Never “pay to play”
- Be suspicious of pressure to wire funds
- Pay attention to warnings from your financial institution
- If the caller claims an emergency, check it out at a number you know to be valid
- Be wary of requests for secrecy

PHANTOM DEBT COLLECTION SCAM



Scammers trick victims into paying a debt that doesn't exist. They may:

- Contact victims via phone
- Refuse to answer any questions
- May have information about victims
- Use threats and scare tactics
- Pose as law enforcement agents or government employees

PHANTOM DEBT COLLECTION SCAM (cont.)

- Refuse to give you a mailing address or phone number
- Ask for personal financial information
- Ask you to buy a prepaid debit card and send the card

DEBT COLLECTION SCAM: SAFEGUARDS

- Ask the debt collector's name, telephone number, and address
- If you don't recognize the debt, ask for more information in writing
- You have the right to get a breakdown of the amount owed
- Don't give any financial or sensitive information
- Keep copies of related papers

SIGNS OF A CHARITY SCAM

Charity scammers:

- Refuse to provide information
- Won’t provide proof that a contribution is tax deductible
- Mimic name of another organization
- Thank you for a pledge that you don’t remember making

SIGNS OF A CHARITY SCAM (cont.)

Charity scammers:

- Pressure victims to donate immediately
- Ask victims to donate cash or wire money
- Request private account info/routing numbers
- Guarantee sweepstakes winning in exchange for a contribution

CHARITY SCAM: SAFEGUARD

- Ask for information (e.g., name, address)
- Research using the organization's name
- Check if the charity is trustworthy (e.g., Wise Giving Alliance, Charity Watch)
- Ask the following from a paid fundraiser:
  - **Name of the charity**
  - **The percentage of your donation that will go to the charity**
- Contact the charity directly about the solicitation

CHARITY SCAM: SAFEGUARD (cont.)

- Keep a record of your donations
- Make an annual donation plan
- Learn if the organization is eligible for tax deductible contributions

Tax deductible:
Contributions to the organization are eligible for tax deduction.

Tax exempt:
The organization doesn't have to pay taxes.

CHARITY SCAM: SAFEGUARD (cont.)

- Pay by check or credit card
- Never send cash donations or wire money
- Do not donate until you've researched the charity
- Be wary of charities that spring up suddenly in response to current events/disasters

COMPUTER/INTERNET SCAMS

Phishing: Authentic-looking emails, text messages, and Web pages to trick unsuspecting users into revealing their personal financial information

Email spoofing:
Email address disguised to look like that of someone you may know

TELL-TALE LANGUAGE

- "*We suspect an unauthorized transaction on your account. To ensure your account is not compromised,* ***please click the link below and confirm your identify****.*"

- "*During our regular verification of accounts, we couldn't verify your information…* ***click here to update and verify your information****.*"

- *"Our records indicate your account was overcharged.* ***Call us to receive your refund****.*"

COMPUTER/INTERNET: SAFEGUARDS

- Use trusted security software and update regularly
- Do not email financial information or account numbers
- Be cautious about opening attachments and downloading files, regardless of the source
- Use passwords that are hard to guess
- Shut down your PC when not using it

COMPUTER/INTERNET: SAFEGUARDS (cont.)

- Do not give control of your computer to a third party
- Do not rely on caller ID alone to authenticate a caller
- Be cautious of scammers posing as tech support online. Use tech support listed on a software package or on your receipt
- Visit onguardonline.gov for more information

RESPOND TO PHISHING ATTACK

- Do not open any message from an unfamiliar sender
- If you open a suspicious message, delete it
- Delete email and text messages that ask you to confirm or provide personal information
- If you are concerned about an account, call the telephone number on your statement

RESPOND TO PHISHING ATTACK (cont.)

If you downloaded malware from a scam tech support:

- Update or download legitimate software and scan your computer
- Delete anything identified as a problem
- Change password

If you paid for bogus tech support services, dispute with your credit card provider.

IDENTITY THEFT

Thieves steal your personal financial information and use your identity to commit fraud and other crimes.

- Social Security Number
- Birth Date
- Credit Card/ Account Numbers
- PINs & Passwords

IDENTITY THEFT: SAFEGUARDS

- Protect your personal information
- Protect incoming and outgoing mail
- Sign up for direct deposit
- Use a shredder to destroy “financial trash”
- Monitor bank accounts and credit card bills
- Avoid come-ons for personal information
- Review your credit record annually and report any fraudulent activity

FRAUD ALERT: SSA

- Scammers attempt to open a fake "*my* Social Security" online account using personal information at ssa.gov
- Scammers are less likely to succeed if you open "*my* Social Security" account yourself

WHO CAN HELP?

If SSA notifies you about opening a "*my* Social Security" account and you didn't open the account, contact

Social Security Customer service

at 1-800-772-1213

TTY: 1-800-325-0778

IDENTITY THEFT: IF YOU ARE A VICTIM

- Place an initial fraud alert with one of the major credit reporting companies
- Request copies of your credit report
- Make an identity theft report
- Consider placing a security freeze on your credit report

IDENTITY THEFT: IF YOU ARE A VICTIM (cont.)

Contact the
Federal Trade Commission:

Identity Theft

- Call 1-877-IDTHEFT (438-4338)
- Visit the FTC at identitytheft.gov

MEDICAL IDENTITY THEFT: WHAT IT IS

Someone steals your personal information *(e.g., your name and Medicare number)* uses it for services, then bills Medicare for:

- Medical treatment
- Prescription drugs
- Surgery or other services

MEDICAL IDENTITY THEFT: RISKS

- It is costly to correct
- Medicare may deny coverage for a service or equipment
- It can affect your medical and insurance records – change your blood type or record a diagnosis for a disease you don’t have
- You could receive wrong, perhaps harmful, treatment

MEDICAL IDENTITY THEFT: WARNING SIGNS

A bill for services you did not receive

Contact from a collection agency for money you do not owe

Notification from insurance company that you have reached your limit for medical benefits

Denial of insurance for a medical condition you don’t have

MEDICAL IDENTITY THEFT: SAFEGUARDS

- Protect your Medicare and insurance cards
- Review Medicare Summary Notices, Explanations of Benefits statements, and medical bills
- Be careful about sharing personal information
- Beware of offers for free equipment, services or goods in exchange for your Medicare number
- Shred papers with your medical identity and destroy prescription labels before throwing in the trash

MEDICAL IDENTITY THEFT: RESPOND

Obtain your medical file

Write to your health plan or provider for correction

Report your concerns to your Senior Medicare Patrol (SMP)

To find your state SMP contact, visit smpresource.org

PLANNING FOR THE UNEXPECTED

Preparing for future health problems or disasters:

- Gives you control
- Relieves stress of decision-making from caretakers and family members
- Saves money and helps avoid financial setbacks
- Allows time to gather information and compare options

PREPARING FOR FUTURE HEALTH PROBLEMS

- Prepare a Plan: review income and expenses
- Make sure trusted family members know where to find necessary documents
- Set up direct deposit for income and benefit checks
- Consider automatic payment of important, recurring bills

PREPARING FOR FUTURE HEALTH PROBLEMS (CONT.)

- Consider a durable power of attorney
- Make sure you are properly insured
- Maintain a healthy lifestyle

RECEIVING SOCIAL SECURITY BENEFITS

Social Security and Supplemental Security Income (SSI) benefit payments:

Direct Deposit

Direct Express® Debit Card

PREPARING FINANCIALLY FOR A DISASTER

What you may need:

Forms of identification

- Driver’s license or government-issued ID
- Insurance cards
- Social Security card
- Passport
- Birth certificate

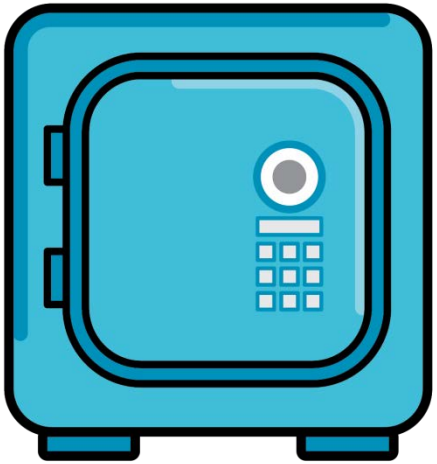
OTHER ITEMS YOU MAY NEED

- Cash
- ATM cards, debit cards, credit cards
- Checkbook (blank checks and deposit slips to last at least a month)
- Phone numbers for financial services providers
- Important account numbers
- Key to safe deposit box

PROTECTING YOUR DOCUMENTS

- Make backup copies of important documents
- Make an electronic image for easy storage
- Give a copy to loved ones or tell them where to find documents in an emergency
- Store backups at a distance from home in case disaster affects entire community
- Make a record of all credit/debit cards with the account and contact numbers to report lost/stolen cards

WHAT TO KEEP; WHERE TO KEEP IT



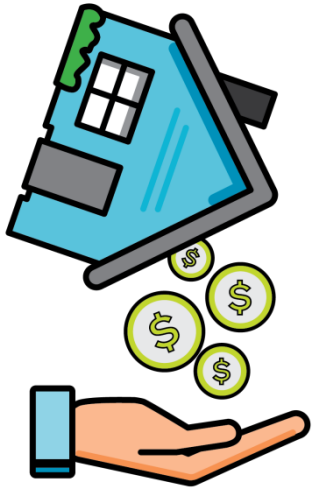
- Store in a safe deposit box
  Birth certificate and originals of important contracts
- Keep at home, preferably in a fireproof safe
  Passport, medical care directives, and will

Seal important documents in airtight, waterproof bags or containers

WHAT ELSE TO CONSIDER

- Prepare emergency evacuation bag(s)
- Arrange for automatic bill payment from your bank account
- Sign up for Internet banking services
- Review your insurance coverage

REVERSE MORTGAGES



Allow homeowners 62 and older to borrow against equity in their homes.

- Monthly interest charges are added to loan amount
- Available as a line of credit, in regular monthly installments, or as a lump sum
- Repayable when you no longer live in the home
- Must maintain the home and pay property taxes and insurance

REVERSE MORTGAGE: SCAMS

- Family members or others pressure a homeowner to get a reverse mortgage so they can “borrow” the money
- Scammer requires borrower to sign a power of attorney or otherwise sign over proceeds
- Brokers pressure borrowers to purchase other financial products

MORTGAGE ASSISTANCE RELIEF SCAM

- Scammers may promise that you can stay in your home or ask for a lot of money to help you
- Scammers might promise guaranteed or immediate relief from foreclosure, and might charge you very high fees for few or no services

CONTRACTOR/ HOME IMPROVEMENT FRAUD

Scam artists use high pressure tactics to sell unneeded and overpriced contracts for "home improvements

CONTRACTOR/ HOME IMPROVEMENT FRAUD

- Promises for quick work at below market prices
- Delivers substandard, unnecessary, or damaging work
- Pressures to pay through threats or intimidation
- May pose as government officials and demand a fee

AVOID CONTRACTOR FRAUD: TIPS

- Verify the identity of anyone claiming to be a government employee
- Obtain written bids from local contractors
- Avoid contractors *who approach you*
- Check for licenses and complaints
- Check references
- Require a clearly written contract
- Don’t pay in advance; never pay cash

AVOID CONTRACTOR FRAUD: TIPS
(cont.)

- Don’t provide personal financial information
- If you need a loan, don’t let the contractor steer you to a lender
- Withhold final payment until you are satisfied and all required inspections are completed

Read *Hiring Contractors* available at consumer.ftc.gov/articles/0242-hiring-contractor

Call 1-877-FTC-HELP (382-4357)

CONCLUSION

You learned about:

- Types of financial exploitation
- Tips for recognizing scams
- Strategies for avoiding identity theft, including medical identity theft
- How to prepare financially for future health problems and disasters