Money Smart Town Hall:
Protecting Older Adults from Scams, Fraud, and Cyber Threats

September 25, 2025

Consumer Financial Protection Bureau

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

U.S. Securities and Exchange Commission

FDIC & CFPB Disclaimer

The Federal Deposit Insurance Corporation (FDIC) and the Consumer Financial Protection Bureau (CFPB) are providing this information as a public service. The views expressed in this presentation are intended for educational purposes only and do not constitute legal, financial, or investment advice, nor do they represent the views of the FDIC or the CFPB.

FDIC FEDERAL DEPOSIT INSURANCE CORPORATION

cfpb Consumer Financial Protection Bureau

Administrative Announcements

Q&A: Ask questions and submit feedback using the Q&A feature.

CAPTIONS: MS Teams offers closed captions, if needed.

EMAIL: ConsumerEducation@fdic.gov if we are unable to address your questions during this program.

This event is being recorded.

Presenters

Deva Tarin

Consumer Education Specialist
Consumer Education
FDIC

Hansen Lasconia

Sr. Consumer Affairs Specialist
Consumer Education
FDIC

Lisa Schifferle

Senior Policy Analyst
Office for Older Americans
cfpb Consumer Financial Protection Bureau

Erin Scheithe

Investor Communication Specialist
Office of Investor Education and Advocacy
U.S. Securities and Exchange Commission

Money Smart for Older Adults

Curriculum Overview

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

cfpb Consumer Financial Protection Bureau

AWARD-WINNING

Money Smart for Older Adults—an award-winning program to prevent scamming and fraud

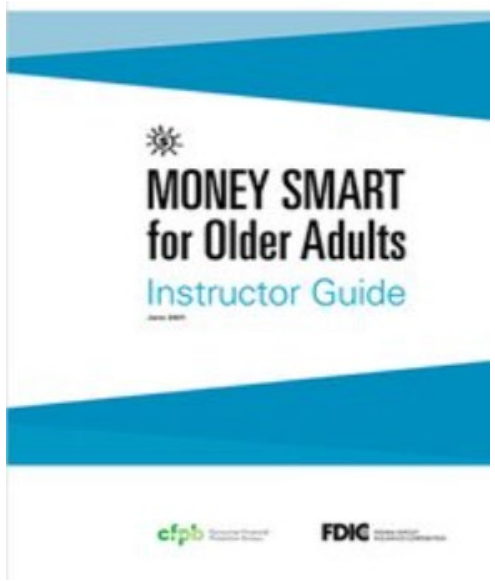
- 2019, American Society on Aging, Gloria Cavanaugh Award for Excellence in Training and Education
- Over 1.5 million copies of MSOA distributed

MONEY SMART FOR OLDER ADULTS

10 Topics

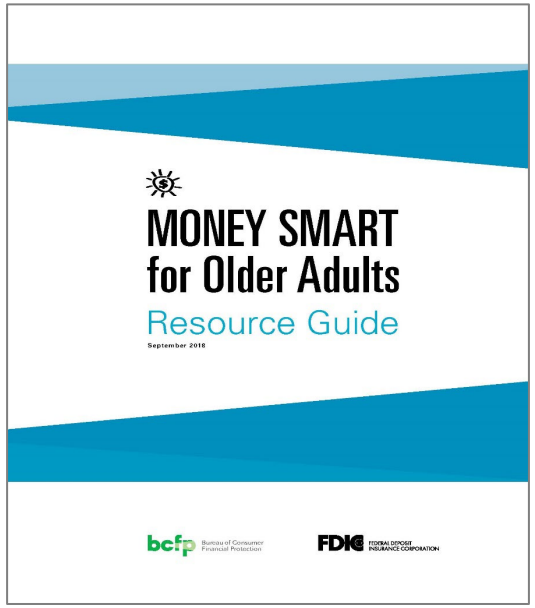
- Common Types of Elder Financial Exploitation
- Investment Fraud
- Avoiding Telephone and Internet Scams
- Avoiding Charity Scams
- Computer-Internet Scams
- Identity Theft and Medical Identity Theft
- Planning for Unexpected Life Events
- Scams that Target Homeowners
- Scams that Target Veterans

COMPONENTS IN EVERY MODULE



Instructor Guide

- ✓ Scripted
- ✓ "Out of the box"
- ✓ No prior teaching or banking experience required



Participant Guide

- ✓ Contains scenarios and activities
- ✓ Pre- and post-surveys
- ✓ Use in classroom training and as a resource at home

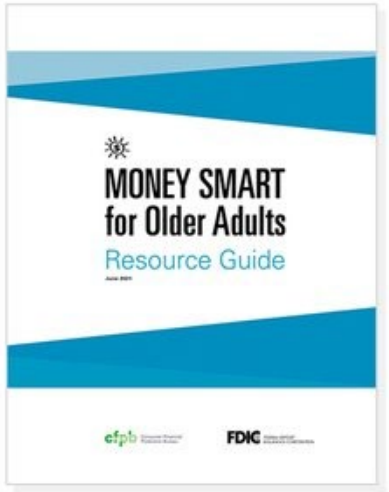
PowerPoint Slides

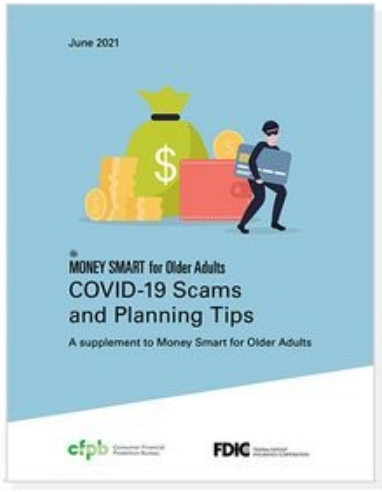
- ✓ Perfectly aligned with the Instructor Guide

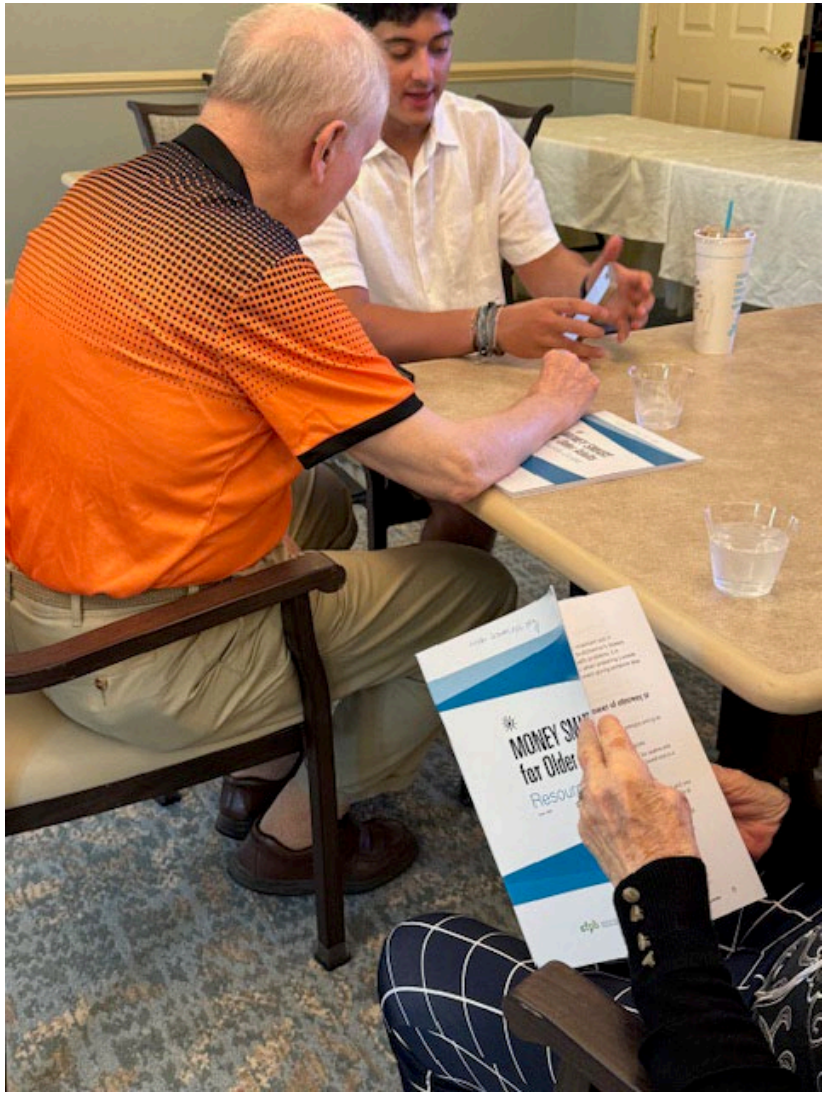
Money Smart in Action!

Success Stories

Scam Cops High School Youth Initiative: AI + MSOA







Background On Elder Financial Exploitation

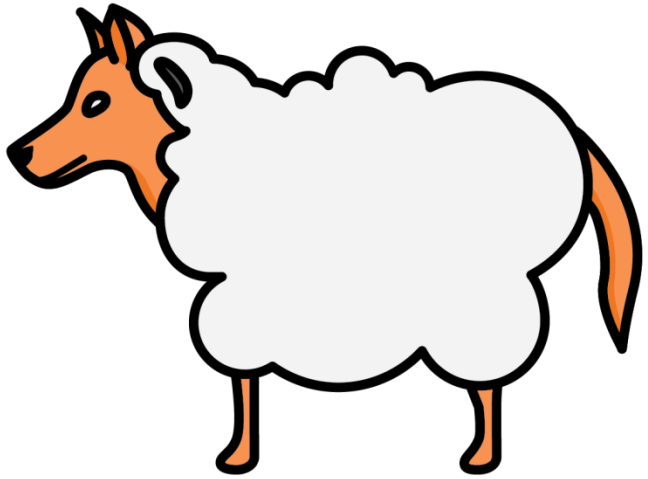
WHAT IS ELDER FINANCIAL EXPLOITATION?

- 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 COULD BE AN ABUSER?

People you know

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



WHO COULD BE AN ABUSER ?

Strangers

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

WHO IS AT RISK?

Anyone can be the victim of financial exploitation.

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

Snapshot Of The Training

Featuring the new content on romance scams

WHAT IS A ROMANCE SCAM?

- A romance scam is when a new love interest says they love you, but they just want your money
- Scammers may:
  - Assume a false identity
  - Take time to build trust with you
  - Ask for money under false pretenses
- The scams can happen online or in person

WHAT SCAMMERS MAY DO

Romance Scammers may:

- Claim they need money for an emergency surgery or medical bill
- Ask for help in paying unexpected customs fees or past gambling debts
- Request money for travel expenses or documentation so that they can visit you
- Seek smaller loan amounts and later ask for larger amounts
- Ask for gift cards and wire transfers (because they are hard to trace and not retractable)

ROMANCE SCAM WARNING SIGNS

A new friend or love interest may:

- Be overly complimentary and flirtatious
- Shower you with attention
- Want you to keep your relationship a secret
- Show unusual interest in your finances
- Try hard to get you to share information about your finances

GETTING HELP

If you lost money to a romance scam:

- Stop communicating with the scammer
- Talk to someone you trust
- Tell your financial institution if you sent money
- Report the scammer to:
  - Local law enforcement
  - Adult Protective Services
  - Federal Trade Commission
- Take action as soon as possible

EXAMPLES OF FINANCIAL EXPLOITATION

Telephone, computer, and internet scams

Identity theft

Lottery and sweepstakes scams

Cyber scams

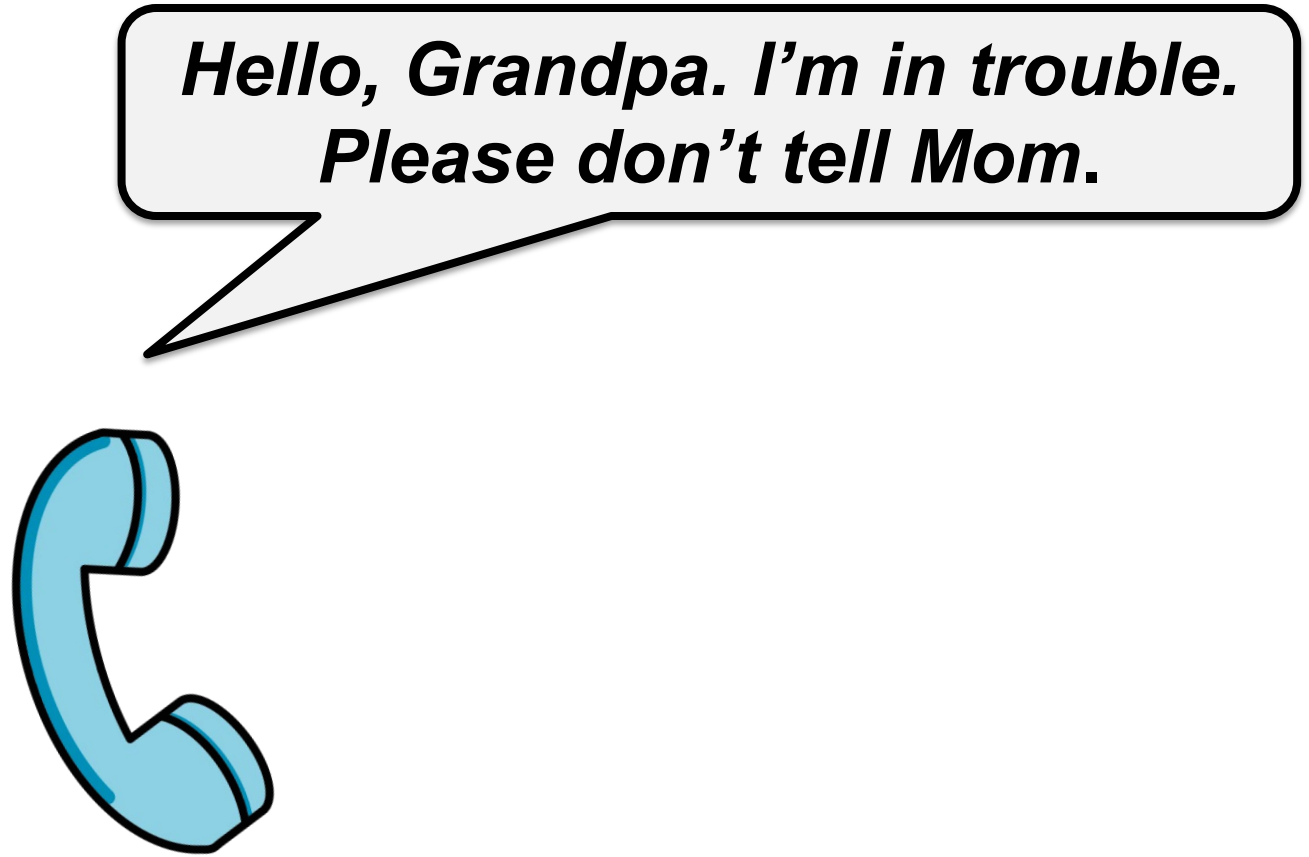
AVOID TELEPHONE AND INTERNET SCAMS

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

GRANDPARENT SCAM

Scammers:

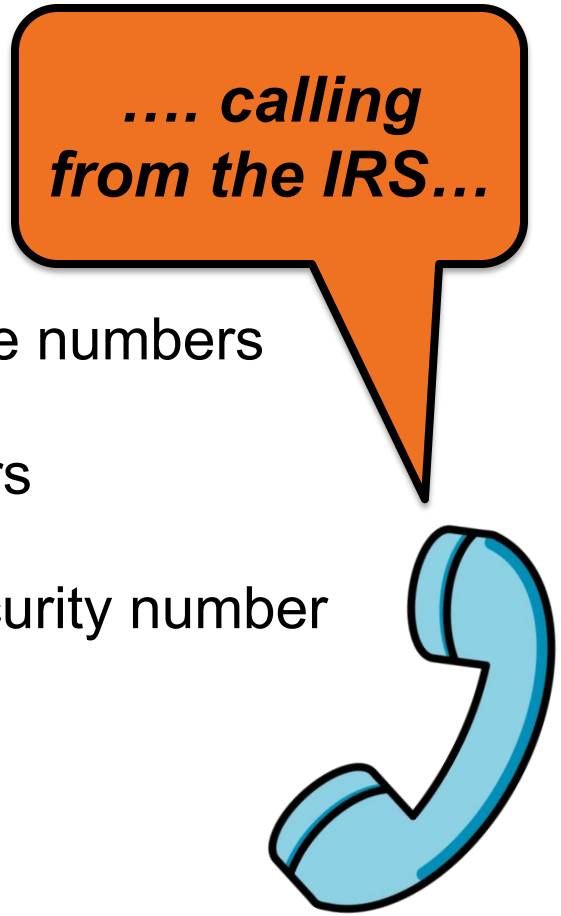
- May know grandchild's name
- Usually cry to disguise voice
- Plead for victim to wire money
- Ask not to tell family members



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



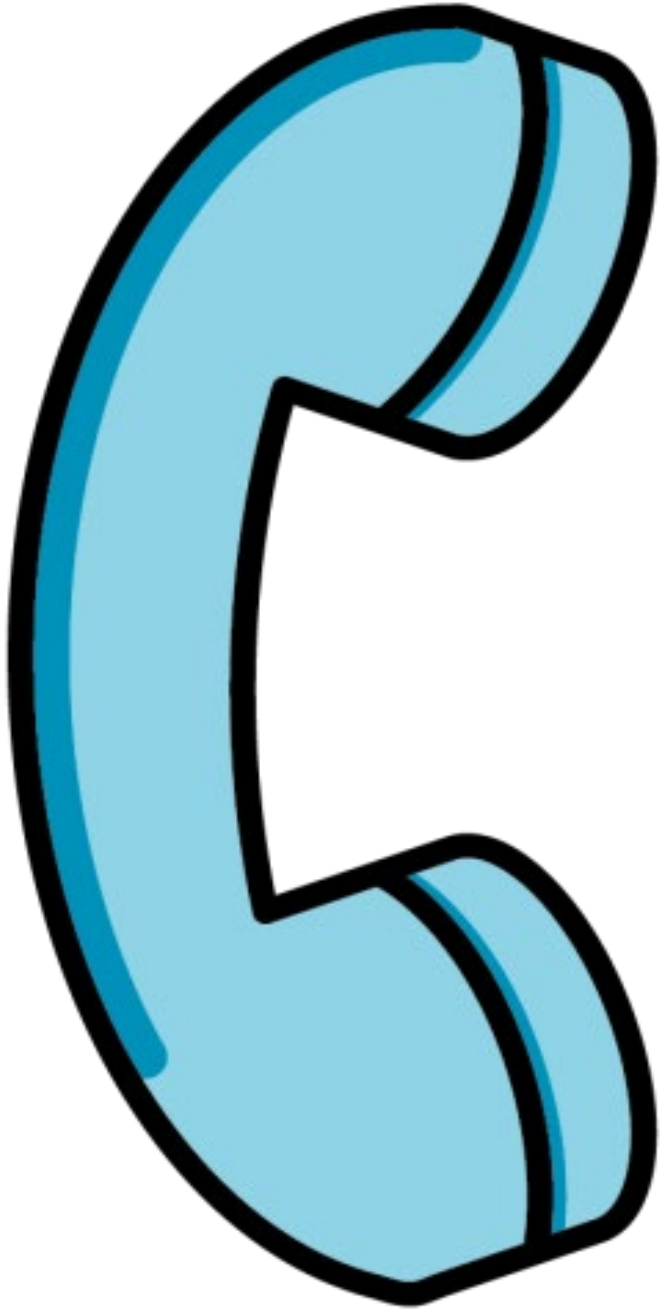
LOTTERY AND SWEEPSTAKES SCAMS

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



ACTIVITY: TELEPHONE SCAMS

- Read each scenario in Scenario 1 in the Resource Guide
- Then, based on what you have learned, answer the questions
- Activity helps participants to identify the red flags of scam scenarios

IDENTITY THEFT

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

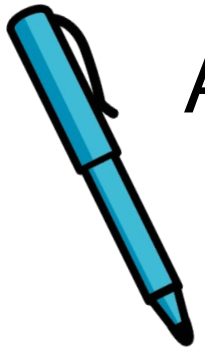
- Social Security Number
- Birth Date
- Credit Card/ Account Numbers
- PINs & Passwords

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

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



ACTIVITY: IDENTITY THEFT

Complete Activity 3 in the Resource Guide.

1. Review each response on the list
2. Indicate how often you perform each action
3. Tally your score to see how well you are taking measures to avoid ID theft

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

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.

FREE RESOURCES

MANAGING SOMEONE ELSE'S MONEY GUIDES

- Help for financial caregivers handling the finances for a family member or another who is unable to do so
- Guides for four types of financial caregivers:
  - Agents under a power of attorney
  - Guardians and conservators
  - Trustees
  - Social Security and Department of Veterans Affairs (VA) representatives

FRAUD PREVENTION PLACEMATS

Consumerfinance.gov/placemats

- Free fraud prevention placemats, handouts, and activity sheets on how to avoid common scams
- Companion resources with tips and information to reinforce the messages

Erin Scheithe

Investor Communication Specialist
Office of Investor Education and Advocacy

U.S. Securities and Exchange Commission

SEC Disclaimer

The SEC's Office of Investor Education and Advocacy is providing this information as a service to investors. This presentation is not a statement of official SEC policy, a legal interpretation, or investment advice.


An official website of the United States government Here's how you know
Investor.gov
U.S. SECURITIES AND EXCHANGE COMMISSION
About Us | Contact Us | Follow Us | Información en Español
Search Investor.gov
Search
Introduction to Investing
Financial Tools & Calculators
Protect Your Investments
Additional Resources
Check Out Your
INVESTMENT PROFESSIONAL
Individual
Name or CRD#
It's a great first step toward protecting your money. Learn about an investment professional's background, registration status, and more.
Quick Links
Never Stop Learning
Resources for Older Investors
Crypto Assets
Financial Tools and Calculators
Understanding Fees
Investing Quizzes

Never stop learning, especially when it comes to protecting your hard-earned money. While we cannot tell you what investments to make or provide legal advice, below we've identified several steps you can consider taking to help protect your assets now and as you age.

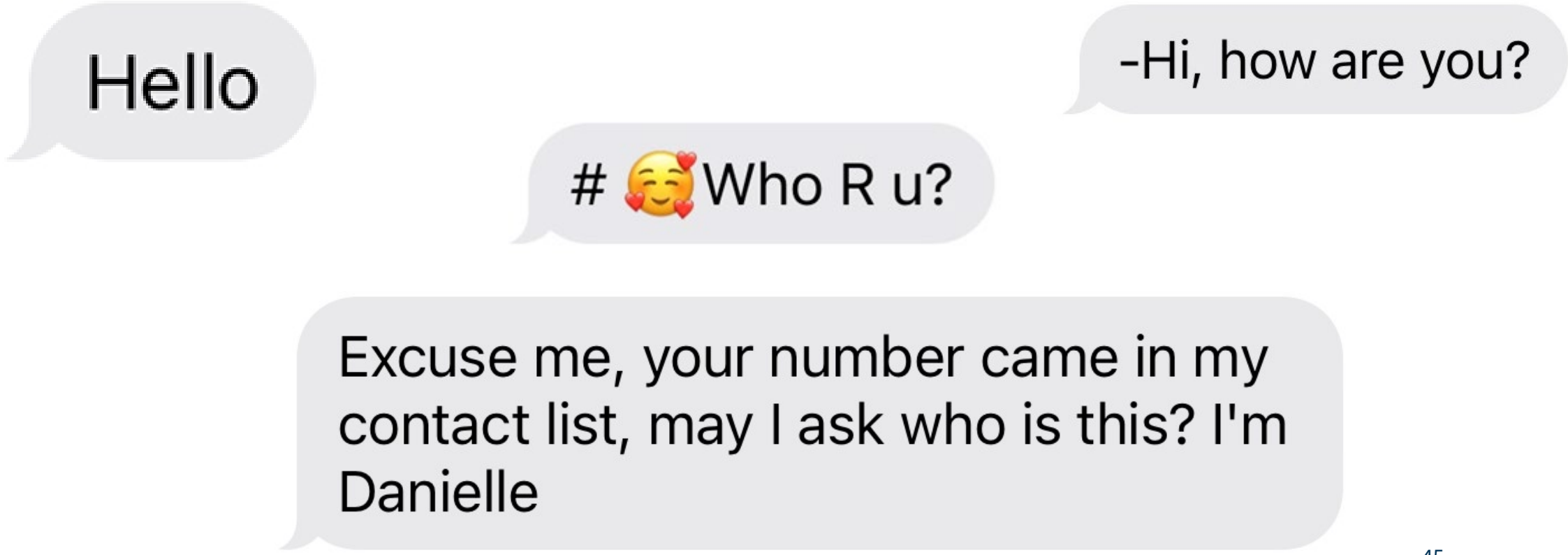
LEARN INVESTING BASICS

Common Investment Scams

- Imposter Scams (including Government Impersonator)
- Advance Fee Fraud
- Relationship Investment Scams
- Pump-and-Dumps
- Affinity Fraud
- Ponzi Schemes
- Pyramid Schemes

Relationship Investment Scams 1 of 2

- Long-term confidence scam that often starts with a wrong number text or a social media message



Relationship Investment Scams 2 of 2

- Scammer develops a relationship with their mark and usually encourages them to invest in crypto assets or other investments
- When the scam blows up, it can be financially and psychologically devastating to the person scammed
- After scam is discovered, the scam may not end – second and third chance for the scammer to take advantage of you through recovery fraud and money mule fraud
- ***Delete, block, report!***

Investor.gov/relationshipscams

Protect Yourself

- Ignore messages from senders you don’t know
- Make investment decisions independent of the advice of someone who contacts you online or through an app or text message
- Research investment opportunities thoroughly
- Don’t share financial or personal information with someone you don’t know
- Never pay money to recover your investment or make an upfront payment to release funds

Stop and Report

- If you think you may be in a relationship scam, stop communicating immediately and don't send more money
- Report any investment scam to the SEC: www.SEC.gov/tcr

Take Steps to Avoid Fraud

- If it sounds too good to be true, it is
- Be careful if you are asked to pay for an investment with gift cards, cryptocurrency, or wires overseas
- Don’t be pressured to buy quickly
- Take your time to do research with unbiased resources
- Testimonials are easy to fake and influencers are often paid to endorse

Contact the SEC

Submit Investor Complaints & Questions:

help.sec.gov or 800-732-0330

Report Suspected Securities Fraud:

www.sec.gov/tcr

Before we continue,
please take 1-2 minutes to share your thoughts.

Subscribe to FDIC Publications

Money Smart News

- FDIC newsletter with Money Smart curriculum tips, updates, and success stories for financial educators.

RECENT ARTICLES

- ✓ Tax Season and Identity Protection | Jan 2025
- ✓ Money Smart and Scams | Dec 2024

FDIC Consumer News

- Practical advice on becoming a smart, safe user of financial services, with helpful hints, tips, and common-sense strategies to protect and stretch your money.

RECENT ARTICLES

- ✓ Scams Targeting Older Adults | July 2025
- ✓ Bank Impersonation Scams and Fake Banks | June 2025

fdic.gov/moneysmart

Money Smart Alliance

Alliance members:

- Provide training
- Promote Money Smart
- Support local organizations that use Money Smart

Benefits of joining include:

- Designated FDIC point of contact
- Option to be listed online in member directory
- Learn from peers across the country (webinars)
- Priority consideration for publication in Money Smart News

Contact us at: MoneySmartAlliance@fdic.gov

Upcoming Event

The FDIC invites you to a national town hall featuring a preview of the redesigned Money Smart for Small Business (MSSB) curriculum. This event will highlight updates to MSSB design, content, interactive tools and how your organization can participate in in pilot testing.

Event Date: October 8, 2025, 2:00 PM- 3:00 PM (Eastern Time)

MONEY SMART Small Business

Register:

Scan the QR code or visit

Money Smart for Small Business (MSSB) Town Hall: A Preview of Upcoming Updates to MSSB | FDIC.gov

Connect with FDIC Money Smart

- Download Money Smart materials and resources, subscribe to Money Smart News and Consumer News, or join the Money Smart Alliance

  fdic.gov/moneysmart

- Comments? Questions?

  ConsumerEducation@fdic.gov

Questions?

ConsumerEducation@fdic.gov

MONEY SMART

Money Smart Town Hall:

Protecting Older Adults from Scams, Fraud, and Cyber Threats.

THANK YOU!

cfpb Consumer Financial Protection Bureau

FDIC FEDERAL DEPOSIT INSURANCE CORPORATION

U.S. Securities and Exchange Commission