Scams and Financial Exploitation: A National Practice Module

Protecting older adults from scams and financial exploitation.

Why this module matters. People 60 and older reported more than $3 billion in fraud losses to the FTC in 2025, and the FTC estimates the true cost could be as high as $119.5 billion.

About this module

This module gives teams a shared, evidence-based approach to protecting older adults from scams and financial exploitation. It draws on current federal rules and national guidance, and it ends with a checklist that agencies, clinicians, and families anywhere in the United States can adopt.

Item	Details
Who it is for	Family caregivers, older adults, home care aides, and agencies
Format	6 units, case scenarios, a knowledge check, and a national checklist
Time	About 1 hour
How to use it	Everyone uses all units. Agencies use the checklist for training.

Learning objectives

After completing this module, learners will be able to:

1. Describe national fraud trends.
2. Recognize the biggest scams.
3. Spot red flags.
4. Prevent scams.
5. Recognize exploitation by known people.
6. Respond and report.

Scope. Aides and family caregivers observe, support, and report. Clinical assessments, medication changes, and legal decisions belong to licensed professionals or qualified advisers. Follow your state rules and agency policies.

Unit 1. The national picture

Measure	Figure	Source
Fraud losses reported to the FTC by people 60+ (2025)	More than $3 billion, up from $2.4 billion in 2024 and $600 million in 2020	FTC, Oct. 2026
FTC estimate of the true cost, including unreported fraud	$13.3 billion to $119.5 billion	FTC, 2026
Losses reported to the FBI by people 60+ (2024)	Nearly $4.9 billion, up 43%	FBI IC3
Complaints to the FBI from people 60+	More than 147,000; average loss $83,000	FBI IC3

Unit 2. The biggest scams

Scam (FTC 2025 losses for people 60+)	Losses	How it works
Investment scams	$1.06 billion, up 42%	Fake crypto or trading opportunities, often starting on social media
Government impersonators	$448 million	Fake IRS, Social Security, Medicare, or police calls demanding payment
Business impersonators	$422 million	Fake bank, Amazon, or tech company alerts
Romance scams	$384 million	Online “partner” who asks for money
Prizes and lotteries	$143 million	“You won, just pay the fees”
Tech support scams	$126 million	Pop-ups or calls about a “virus”

The FTC found that the largest losses were paid by bank transfer ($1.03 billion) and cryptocurrency ($603 million), followed by cash, wire transfers, and gift cards.

Unit 3. Red flags

- ☐ Pressure to act right now, or keep it secret.
- ☐ A request to pay by gift card, crypto, wire, cash courier, or a payment app.
- ☐ A caller says your account is compromised and you must move money to “keep it safe.”
- ☐ Someone you have never met in person asks for money.
- ☐ You must pay to collect a prize.
- ☐ A government agency threatens arrest by phone.
- ☐ A pop-up says to call a number to fix your computer.

Unit 4. Prevention

Step	How
Hang up and verify	Call the bank or agency using the number on the card or official website
Never share codes	Do not give one-time passcodes, passwords, or remote access
Slow down	Talk to someone you trust before sending money
Set up protections	Bank alerts, a trusted contact on accounts, credit freeze, call blocking
Limit public information	Tighten social media privacy
Guard mail and documents	Shred papers with account information

Unit 5. Financial exploitation by people the person knows

Exploitation is not only by strangers. Family members, friends, or caregivers can misuse money, property, or a power of attorney.

- Unexplained withdrawals or missing belongings.
- New names on accounts or documents.
- Unpaid bills despite enough income.
- The person seems afraid of, or isolated by, someone.

Report concerns to Adult Protective Services, the bank, and law enforcement. Caregivers may be mandated reporters.

Unit 6. If it happens

1. Stop contact and do not send more money.
2. Call the bank or payment company immediately to try to stop or reverse payments.
3. Change passwords; check credit reports.
4. Report to the FTC (ReportFraud.ftc.gov) and the FBI (ic3.gov).
5. Call the National Elder Fraud Hotline: 1-833-FRAUD-11 (1-833-372-8311).
6. Report to local police and Adult Protective Services.
7. Watch for “recovery” scams promising to get money back for a fee.

> **Be kind.** Victims often feel ashamed. Respond with support, not blame. Scammers are professionals.

Case scenarios

Case 1. “Your account is hacked”

Mrs. K gets a call from “her bank” telling her to move savings to a “safe account.”

- What are the red flags?
- What should she do?

Discussion: Urgency and a request to move money. Hang up and call the bank using the number on her card.

Case 2. A new online friend

Mr. L met someone online who now needs money for a “medical emergency” overseas.

- What should family do?

Discussion: Talk calmly, explain romance scams, avoid blame, and report to the FTC and FBI if money was sent.

Knowledge check

1. How much did people 60+ report losing to the FTC in 2025? *(More than $3 billion)*
2. Which scam caused the most FTC-reported losses? *(Investment scams)*
3. Name three red-flag payment methods. *(Gift cards, crypto, wire, cash courier)*
4. What is the National Elder Fraud Hotline? *(1-833-372-8311)*
5. Where do you report suspected exploitation by someone known? *(Adult Protective Services, the bank, and law enforcement)*

National Scam and Financial Exploitation Prevention Checklist

This checklist turns FTC and FBI guidance into one tool for families, caregivers, and agencies. The "National basis" column shows where each item comes from. Adapt it to your state rules and policies.

Name or ID	Date	Completed by and role
Agency or organization	Reviewed by	Next review date

A. Protect

Action	National basis	Done	Notes
Bank alerts and trusted contact set up	FTC; CFPB	☐	
Credit freeze considered	FTC	☐	
Call blocking and spam filters on	FTC	☐	
"Hang up and verify" rule agreed	FTC	☐	

B. Watch

Action	National basis	Done	Notes
Caregivers trained on scam red flags	FTC; FBI IC3	☐	
Unusual account activity reviewed	Best practice	☐	
Signs of exploitation by known people watched	Elder justice practice	☐	

C. Respond

Action	National basis	Done	Notes
Bank or payment company called immediately	FTC	☐	
Reported to FTC and FBI IC3	FTC; FBI	☐	
National Elder Fraud Hotline called	U.S. Department of Justice	☐	
APS and police notified when appropriate	State law	☐	

Completed by: signature	Printed name and title	Date
Reviewed by: signature	Printed name and title	Date

Sources and further reading

PPC Land: FTC Protecting Older Consumers 2025–2026 report (Oct. 2026) (ppc.land)

AARP: FBI report on 2024 fraud losses (aarp.org)

This resource is for general education. It is not legal advice and does not replace your state rules, your license requirements, or your agency policies. You may print, copy, and adapt it for non-commercial use. Please keep the credit to Aricares Alliance. Questions or corrections: contact@aricaresalliance.com.