

# Addressing Fraud and Scams in APS Service Plans

INSTRUCTOR LED TRAINING  
TRAINER MANUAL



The Academy for Professional Excellence is a project of the San Diego State University School of Social Work

## Funding Sources



**This training was developed by the Academy for Professional Excellence, with funding from the California Department of Social Services, Adult Programs Division.**

**Curriculum Developers, 2025**

**Cynthia Carlson, MSSW, LICSW, Adult Protection Supervisor**

**Thomas Holt, PhD**

© 2025 Academy for Professional Excellence. All rights reserved.

## Table of Contents

Funding Sources.....	1
Table of Contents .....	2
Introduction.....	5
Partner Organizations .....	6
Acknowledgements .....	7
How to Use This Manual .....	8
Trainer Guidelines .....	9
Virtual Training Tips.....	11
Executive Summary .....	13
Course Outline .....	14
<b>Welcome, Introductions and Course Overview .....</b>	<b>18</b>
Slide #1: Addressing Frauds and Scams in APS Service Plans .....	19
Slide #2: Welcome and Introductions .....	20
Slide #3-5: Land Acknowledgement .....	21
Slide #6: Housekeeping .....	23
Slide #7: Learning Objectives .....	24
Slide #8: Introduction to “Fraud” and “Scams” .....	25
Slide #9: At the Watercooler Scams Chat.....	27
<b>Types and Impact of Fraud .....</b>	<b>29</b>
Slide #10: Fraud and Manipulation .....	30
Slide #11: Common Risk Factors for Fraud Victimization .....	32
Slide #12: Warning Signs of Fraud Victimization .....	34
Slide #13: Fraud Types: Phone Scams – How They Work .....	35
Slide #14: Fraud Types: Phone Scams – Red Flags .....	37
Slide #15: Fraud Types: Emergency Scams – How They Work .....	38
Slide #16: Fraud Types: Emergency Scams – Red Flags .....	40
Slide #17: Fraud Types: Phishing/Smishing – How They Work .....	41
Slide #18: Fraud Types: Phishing/Smishing – Red Flags .....	43
Slide #19: Fraud Types: Romance Scams – How They Work.....	45

Slide #20: Fraud Types: Romance Scams – Red Flags .....	47
Slide #21: Fraud Types: Investment Fraud – How They Work.....	49
Slide #22: Fraud Types: Investment Fraud – Red Flags .....	51
Slide #23: Consequences of Fraud: Word Cloud .....	53
Slide #24: Consequences of Fraud: Financial Harm .....	54
Slide #25: Consequences of Fraud: Emotional Harm .....	55
Slide #26: Consequences of Fraud Victimization: Health and Social.....	57
Slide #27: Resource Mapping .....	59
Handout: Fraud Recovery Resource Mapping Worksheet .....	61
<b>Neurocognitive Ability and Susceptibility Factors.....</b>	<b>62</b>
Slide #28: Correlation Between Fraud and the Brain.....	63
Slide #29: Changes in Neurocognition and Decision-Making .....	64
Slide #30: How Brain Changes Impact Scam Susceptibility .....	65
Slide #31: Brain Region Match-Up.....	66
Slide #32: Additional Cognitive Vulnerabilities .....	68
Slide #33: Loneliness and Fraud Susceptibility.....	69
Slide #34: Exploring the Digital Landscape.....	71
Slide #35: Barriers To Reporting .....	73
<b>Person-Directed Service Planning .....</b>	<b>75</b>
Slide #36: Effective Communication with Clients.....	76
Slide #37: Motivational Interviewing-Inspired Approaches .....	78
Slide #38: Introduction to Service Planning.....	80
Slide #39: Fraud Recovery Service Planning .....	82
Handout: Fraud Recovery Service Planning.....	84
Slide #40: The Scams Inverted Intervention Triangle .....	85
Slide #41: Harm Reduction .....	87
Slide #42: Cognitive and Behavioral Strategies.....	90
Slide #43: Interventions for Clients with Decision-Making Ability .....	92
Slide #44: Interventions for Clients Without Decision-Making Ability .....	94
Slide #45: Activity – Without Decision Making Ability.....	96
Slide #46: Applying These Skills to Fraud Cases .....	97

Handout: Case Scenarios .....	101
<b>Wrap-Up .....</b>	<b>104</b>
Slide #47: Review and Summary .....	105
Slide #48: P.I.E. ....	107
Slide #49: Evaluations.....	108
Appendix: Resource Handout .....	109
References .....	111

## Introduction

We are pleased to welcome you to **Addressing Fraud and Scams in APS Service Plans, Trainer Manual** developed by Adult Protective Services Workforce Innovations (APSWI), a program of the Academy for Professional Excellence under a grant from the California Department of Social Services, Adult Programs Division.

The Academy for Professional Excellence, a project of San Diego State University School of Social Work, was established in 1996 with the goal of revolutionizing the way people work to ensure the world is a healthier place. Our services integrate culturally responsive and recovery-oriented practices into our daily work to promote healing and healthy relationships. Providing around 70,000 learning experiences to health and human service professionals annually, the Academy provides a variety of workforce development solutions in Southern California and beyond. With five programs, three divisions and over 100 staff, the Academy's mission is to provide exceptional learning and development experiences for the transformation of individuals, organizations and communities.

APSWI is a program of the Academy for Professional Excellence. APSWI is designed to provide competency-based, multidisciplinary training to Adult Protective Services professionals and their partners. APSWI's overarching goal is the professionalization of Adult Protective Services professionals to ensure that abused and vulnerable older adults and adults with disabilities receive high quality, effective interventions and services.

APSWI partners with state and national organizations and experts in the older adult and adults with disabilities professions to empower APS professionals and those they serve to live safely, peacefully and in a world that is free from abuse and neglect.

APSWI's partners include:

- National Adult Protective Services Association (NAPSA) and the National Adult Protective Services Training Center (NATC)
- California Department of Social Services (CDSS), Adult Programs Division
- County Welfare Directors Association of California (CWDA), Protective Services Operations Committee (PSOC)
- California's Curriculum Advisory Committee (CAC) Committee

## Partner Organizations

### **Dawn Gibbons-McWayne, Program Director, APSWI**

Academy for Professional Excellence

<https://theacademy.sdsu.edu/programs/apswi/>

### **Kat Preston-Wager, Workforce Development Supervisor, APSWI**

Academy for Professional Excellence

<https://theacademy.sdsu.edu/programs/apswi/>

### **Alexandra Ernst, Workforce Development Specialist, APSWI**

Academy for Professional Excellence

<https://theacademy.sdsu.edu/programs/apswi/>

### **Jennifer Spoeri, Executive Director, National Adult Protective Services Association (NAPSA)**

<https://www.napsa-now.org/>

### **Paul Needham, Chair, NAPSA Education Committee**

<https://www.napsa-now.org/>

### **James Treggiari, Adult Protective Services Liaison, Adult Protective Services Division**

California Department of Public Social Services

<https://www.cdss.ca.gov/adult-protective-services>

### **Jason Kemp Van Ee and Emily Nicholl, Co-Chairs, Protective Services Operations Committee of the County Welfare Director's Association (PSOC)**

<https://www.cwda.org/about-cwda>

## Acknowledgements

This training is the result of a collaborative effort between Adult Protective Services administrators, supervisors, staff development officers and line staff across the state and the nation; professional educators; and the Academy for Professional Excellence staff members. APSWI would like to thank the following individuals and agencies:

### **Agencies**

California Department of Social Services, Adult Programs Division

National Adult Programs Services Training Center

National Adult Protective Services Association

### **Committees:**

California's Curriculum Advisory Committee with input provided by:

- Quatana Hodges, Social Services Supervisor, Orange County
- Whitney Barnes, MSW, Social Work Supervisor, Santa Cruz County
- Katie Wilson, Instructional Designer, NAPSA
- Amanda Servin, Social Work Supervisor, San Luis Obispo County

Southern California's Training Planning Committee

National Adult Protective Services Association (NAPSA) Education & Development Committee

### **Curriculum Developers**

Cynthia Carlson, MSSW, LICSW, Adult Protection Supervisor

Thomas Holt, PhD



## How to Use This Manual

This curriculum was developed as a virtual **4-hour workshop, excluding breaks**, using the Zoom platform, paying close attention to virtual training best practices. It can be tailored to a different virtual platform (WebEx, GoTo Training, etc.), if necessary. It may also be trained in-person by modifying activity and engagement prompts as necessary. When possible, virtual and in-person prompts are given. If desired, this workshop could be broken into shorter sessions.

The Participant Manual should be sent ahead of time as a fillable PDF if using Adobe Acrobat or to allow participants to print a hard copy.

- Actions which the trainer takes during the training are written in **bold**
- *Trainer notes are italicized*

**Use of language:** Throughout the manual, APS professional is used to denote individual staff who may go by various titles. The term client is used most often to describe the individual at the center of the APS investigation. However, if concept or material was directly quoted from copyrighted material, another term may be used.

He and she have been replaced with the gender-neutral they throughout this manual, unless quoted from copyrighted material. This should not be thought of as plural persons, but rather a gender-neutral term describing all humans.

### **Customizing the Power Point:**

This manual is set up so that the trainer script/ background material is on the same page as the accompanying PowerPoint slide. **Hide a slide instructions:**  
1. On the Slides tab in normal view, select the slide you want to hide.

On the Slide Show menu, click Hide Slide. The slide number will have a line through it to show you have hidden it.

NOTE: The slide remains in your file even though it is hidden when you run the presentation.

The course outline, provided in the next section of this manual, is the class schedule used for development of this curriculum. It can be used to help determine how much time is needed to present each section. However, times will vary based on the experience and engagement of the audience.

## Trainer Guidelines

It is recommended that this workshop be facilitated by someone with expertise in both APS services planning and scams prevention and response. If a single trainer does not hold both areas of expertise, co-facilitation is encouraged—ideally pairing an APS professional with a scams and fraud specialist to ensure comprehensive coverage of the material.

Suggestions for virtual training when possible:

- Have a moderator or co-host who can primarily focus on the virtual aspects of this training (e.g., monitoring chat box, launching polls, assigning breakout groups, monitoring participant reactions, etc.).
- Test out the use of the breakout room feature prior to conducting this training.
- Log in at least 30 minutes prior to the training to ensure the virtual classroom is fully functioning and that you are comfortable navigating it.
- Your equipment and platform may dictate how you do some activities or discussion. There are times you may not be able to see everyone's faces, names or reactions (thumbs up, mute/unmute, etc.). There is a need for both verbal discussion and chat discussion. At such times, the moderator will fill a critical role monitoring those features you cannot. Practice during a run through how you will use the various functions for each section.
- The optimal size for this virtual training is 25-30 participants.

<b>Teaching Strategies</b>	<p>The following instructional strategies are used:</p> <ul style="list-style-type: none"> <li>○ Lecture segments</li> <li>○ Interactive exercises (e.g., breakout groups, chat box discussion, video demonstration, polling activities)</li> <li>○ Question/answer periods</li> <li>○ PowerPoint Slides</li> </ul>
----------------------------	---

<b>Materials and Equipment</b>	<b>The following materials are provided and/or recommended:</b> <ul style="list-style-type: none"><li>○ Trainer Manual</li><li>○ Participant Manual (fillable PDF)</li><li>○ PowerPoint Slides</li><li>○ Headset with microphone Computer</li></ul>
--------------------------------	---

## Virtual Training Tips

Training and facilitation have always been an art. Virtual training is no exception. Below are some helpful tips to remember and implement when training in a virtual environment.

- Assume nothing.
  - Do not assume everyone has the same knowledge or comfort level with technology or has access to equipment like printers, video camera, headsets or even reliable Wi-Fi.
- Distractions are everywhere.
  - Participants have greater access to distractions (email, phone, others at home) which can take their focus away from the training. Therefore, explain everything and summarize before asking participants to complete an activity and check for clarification.
- Over explain when possible.
  - The virtual room doesn't allow for participants to see everything you're doing as they can in-person. Share as you navigate the virtual environment. If you are silent while looking for something or finding a screen, they may think something is frozen.
- Mute with purpose.
  - "Mute all" function can help ensure we don't hear conversations we're not supposed to. However, it can also send a message to the participants that they are a passive participant and may not make them feel comfortable taking themselves off mute when you want them to speak.
- Two screens can be a lifesaver.
  - This allows you to move your chat box or participant gallery view away from your presentation so you can see more of what's going on.
- Rely on practice, not luck.
  - Winging it during an in-person training or facilitation may work from time to time, but doesn't work in the virtual environment. In addition to covering the content, you have to manage all of the technology issues, learning styles in a virtual room, and it will show if you're not prepared.
- Bring the energy.
  - As trainers, we are no strangers to being "on," standing and moving around. However, some of the body language, subtle nonverbal skills we relied on the in-person training room do not translate well in the virtual environment. While this may make you more tired, it's

- important to up your enthusiasm, voice, and presence in order to engage with attendees.
- Be mindful of your space.
    - Training virtually brings an entirely new component of what we're willing to share with others. Learners can get distracted with what's in your background, whether what is physically there or if you set your video to use a virtual background.
    - It's important to reflect on questions of privilege, diversity and equity when thinking of your training space.

## Executive Summary

Fraud and scams targeting older and dependent adults are growing in complexity and impact, often leaving those who have been scammed or defrauded with emotional, financial, and social harm that can be difficult to recover from. Scammers exploit unique vulnerabilities that older adults and adults with cognitive disabilities face such as changes in cognition, emotional processing, and social isolation. This training offers Adult Protective Services professionals a practical understanding of how these schemes operate, why they are so effective, and how to respond with empathy and skill.

Throughout this course, participants will explore the psychological, neurological, and social dynamics that increase scam susceptibility, will examine a wide range of fraud types, and explore how technology and social engineering play a central role in these schemes. The training also highlights the emotional toll of fraud, including shame, grief, and fear, and emphasizes the importance of trauma-informed care and person-directed service planning.

Participants will leave the course equipped with strategies to support clients through recovery and prevention. By integrating case studies, interactive discussions, and evidence-based practices, this training empowers APS professionals to respond to fraud with compassion, clarity, and confidence, ensuring that those they serve are protected, supported, and respected.

### **Instructor Led Training**

This course is an Instructor Led Training, designed to be facilitated virtually. The curriculum and activities can be adapted to an in-person environment with the appropriate materials.

### **Intended Audience**

This training is intended for new and experienced APS professionals who interview clients and collaterals, provide risk assessments, and develop service plans.

### **Course Requirements**

Participants should have some practice with interviewing and service planning.

### **Learning Objectives:**

Upon completion of this training, participants will be able to:

- Recognize prevalent types of scams impacting the APS client population and the role of technology and social engineering used.
- Describe the psychological, cognitive, and social factors that increase scam susceptibility and barriers to reporting.
- Identify effective interventions to support person-directed service planning.

## Course Outline

CONTENT	MATERIALS	TIME
<b>Welcome, Introductions, Overview</b>	Slides 1-9	<b>Total: 25 minutes</b>
Welcome and Introductions		
About the Academy and APSWI		
Land Acknowledgement		
Technology & Housekeeping		
Learning Objectives & Course Overview		
Introducing “Scams” and “Fraud”		
<i>Activity: “Water Cooler” Breakout Groups</i>		5-10 minutes
<b>Types and Impacts of Fraud</b>	Slide 10-27	<b>Total: 75 minutes</b>
Fraud and Manipulation <i>Activity: Everyday Assumptions, Everyday Risks</i>		5-10 minutes
Common Characteristics of Fraud Victimization		
Warning Signs of Fraud/Scam Victimization		
Fraud Types: Phone Scams – How They Work		
Fraud Types: Phone Scams – Red Flags		

<b>CONTENT</b>	<b>MATERIALS</b>	<b>TIME</b>
Fraud Types: Emergency Scams – How They Work		
Fraud Types: Emergency Scams – Red Flags		
Fraud Types: Phishing/Smishing – How They Work		
Fraud Types: Phishing/Smishing – Red Flags		
Fraud Types: Romance Scams – How They Work		
Fraud Types: Romance Scams – Red Flags		
Fraud Types: Investment Fraud – How They Work		
Fraud Types: Investment Fraud – Red Flags		
<i>Activity: Consequences of Fraud: Word Cloud</i>		5 minutes
Consequences of Fraud Victimization: Financial Harm		
Consequences of Fraud Victimization: Emotional Harm <i>Activity: Emotional Impact Reflection</i>		5 minutes
Consequences of Fraud Victimization: Health and Social		
Resource Mapping	Handout: Fraud Recovery Resource	15 minutes



CONTENT	MATERIALS	TIME
<i>Activity: Identifying Public and Private Supports for Fraud Recovery</i>	Mapping Worksheet	
<b>Neurocognitive Ability and Susceptibility Factors</b>	<b>Slides 28-35</b>	<b>Total: 45 minutes</b>
Correlation Between Fraud and the Brain		
Changes in Neurocognition and Decision-Making		
How Brain Changes Impact Scam Susceptibility		
<i>Activity: Brain Region Match-Up</i>		5-7 minutes
Additional Cognitive Vulnerabilities		
Loneliness and Fraud Susceptibility		
<i>Activity: Technology, Connection, and Risk – Exploring the Digital Landscape of Older Adults</i>		10 minutes
Barriers to Reporting		
<b>Person-Directed Service Planning</b>	<b>Slides 36-46</b>	<b>Total: 80 minutes</b>
Effective Communication Strategies		
Motivational Interviewing-Inspired Approaches		
Introduction to Service Planning		

CONTENT	MATERIALS	TIME
Fraud Recovery Service Planning	Handout: Fraud Recovery Service Planning	
The Scams Inverted Intervention Triangle		
Harm Reduction <i>Activity: Interventions Brainstorm – Least to Most Restrictive</i>		10-15 minutes
Cognitive and Behavioral Strategies		
Interventions for Clients with Decision-Making Ability		
Interventions for Clients Without Decision-Making Ability		
<i>Activity: Without Decision-Making Ability</i>		5 minutes
<i>Activity: Applying Skills to Fraud Cases</i>	Handout: Case Scenarios	20-30 minutes
<b>Wrap-Up</b>	<b>Slides: 47-49</b>	<b>Total: 15 minutes</b>
Review and Summary		
P.I.E.		5 minutes
Evaluations & Thank You		
<b>TOTAL (Excluding Breaks)</b>		<b>4 hours</b>

## Welcome, Introductions and Course Overview

**Time Allotted:** 25 Minutes

**Associated Objective(s):** N/A

**Method:** Instruction, Small Breakout Groups

---

## Slide #1: Addressing Frauds and Scams in APS Service Plans

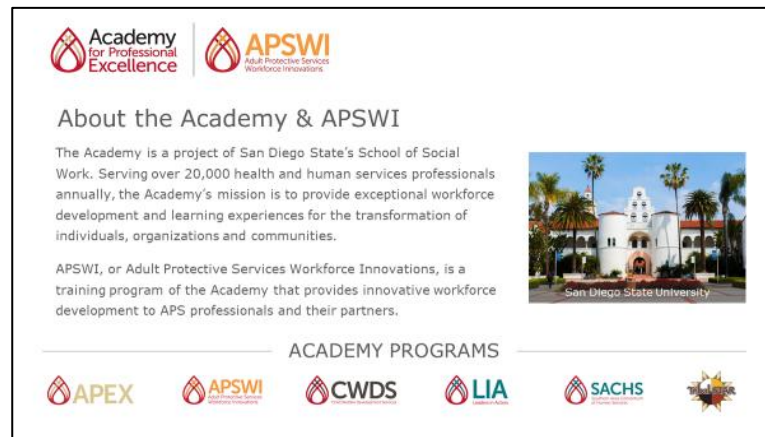


**Welcome** participants and allow everyone to settle in.

**Ask** participants to sign in or type names, titles, and counties into chat box.

**Provide** participants with Participant Manual.

## Slide #2: Welcome and Introductions



**Academy for Professional Excellence** | **APSWI** Adult Protective Services Workforce Innovations


### About the Academy & APSWI

The Academy is a project of San Diego State's School of Social Work. Serving over 20,000 health and human services professionals annually, the Academy's mission is to provide exceptional workforce development and learning experiences for the transformation of individuals, organizations and communities.

APSWI, or Adult Protective Services Workforce Innovations, is a training program of the Academy that provides innovative workforce development to APS professionals and their partners.

San Diego State University

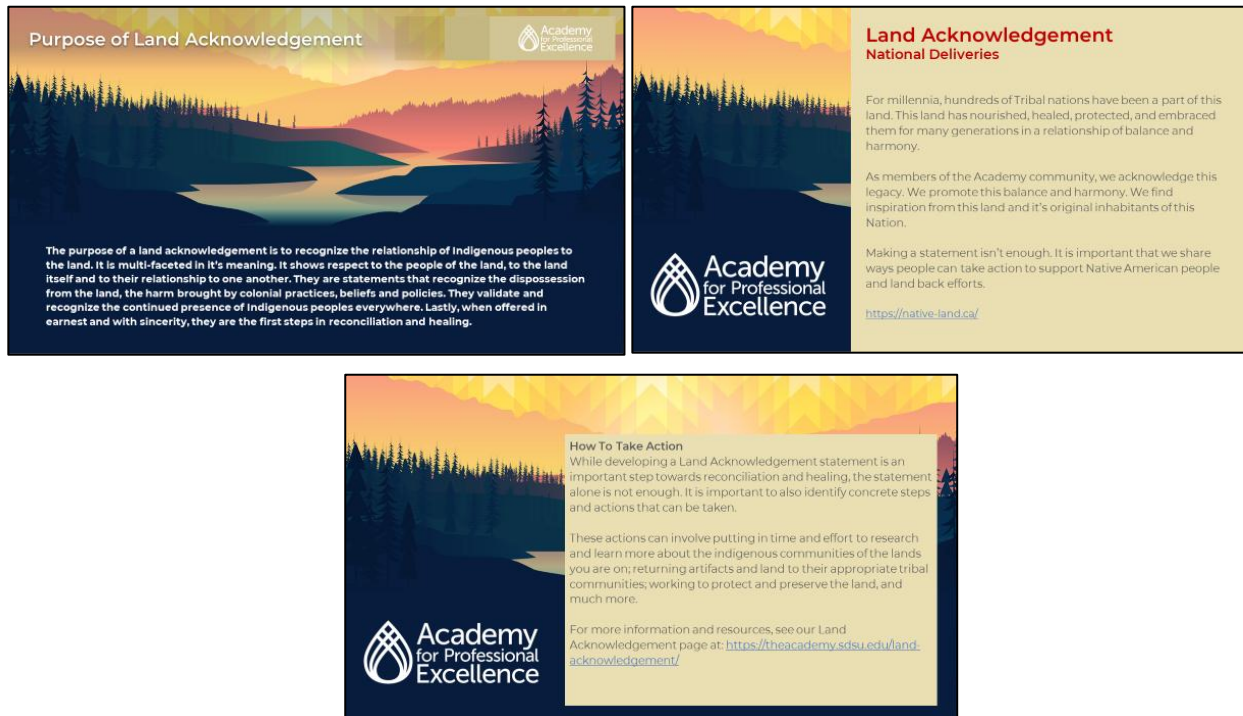
#### ACADEMY PROGRAMS

**APEX** | **APSWI** | **CWDS** | **LIA** | **SACHS** | 

**Explain** that the Academy for Professional Excellence is a project of San Diego State School of Social Work. Its mission is to provide exceptional workforce development and learning experiences for the transformation of individuals, organizations, and communities.

**Explain** that Adult Protective Services Workforce Innovations (APSWI) provides innovative workforce development to APS professionals and their partners. APSWI is a program of the Academy for Professional Excellence along with others listed on the slide.

## Slide #3-5: Land Acknowledgement



**Explain** that the Academy for Professional Excellence is a project of San Diego State School of Social Work. Its mission is to provide exceptional workforce development and learning experiences for the transformation of individuals, organizations, and communities.

- **Explain** that Adult Protective Services Workforce Innovations (APSWI) provides innovative workforce development to APS professionals and their partners. APSWI is a program of the Academy for Professional Excellence along with others listed on the slide. Slide #5- How To Take Action. Making a statement isn't enough. It is important to also identify concrete steps and actions that can be taken to support Native American people including land back efforts which are necessary steps towards reconciliation and healing. These actions can involve putting in time and effort to research and learn more about the indigenous communities of the lands you are on; returning artifacts and land to their appropriate tribal communities; working to protect and preserve the land, and much more.
- **Share:** For millennia, hundreds of Tribal nations have been a part of this land. This land has nourished, healed, protected, and embraced them for many generations in a relationship of balance and harmony. As members of the Academy community, we acknowledge this legacy. We promote this

balance and harmony. We find inspiration from this land; the land of the original inhabitants of this Nation. Find the tribe(s) in your area:

<https://native-land.ca/>

## Slide #6: Housekeeping



**Cover** any housekeeping items, including virtual technology if needed. Some items may include:


- Agenda
- Length of course
- Breaks
- Expectations and agreements of participation



## Slide #7: Learning Objectives

**Learning Objectives**

- Recognize prevalent types of scams impacting the APS client population and the role of technology and social engineering used.
- Describe the psychological, cognitive, and social factors that increase scam susceptibility and barriers to reporting.
- Identify effective interventions to support person-directed service planning.



**Review** the following:

Upon completion of this training, participants will be able to:

- Recognize prevalent types of scams impacting the APS client population and the role of technology and social engineering used.
- Describe the psychological, cognitive, and social factors that increase scam susceptibility and barriers to reporting.
- Identify effective interventions to support person-directed service planning.

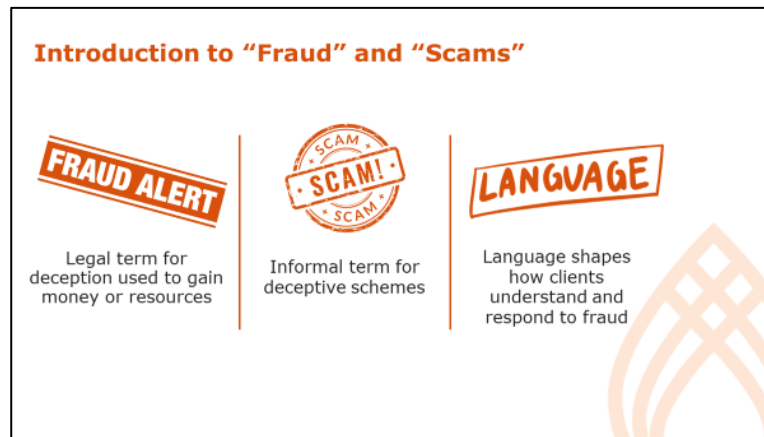
**Share** that at any point, fraudsters are attempting to scam any of us, no matter our age, education, origin, etc. This workshop will explore some of the most prevalent fraud schemes occurring online and through technology, with a focus on how these scams operate and why they are often directed toward older adults and adults with cognitive disabilities.

**Note** that some of the early content, such as scam tactics and emotional manipulation, is designed not only to support APS professionals in their work, but also to help them recognize and respond to scams in their own lives. These insights are applicable both professionally and personally, and we'll highlight "what this means for APS" throughout the training.

**Note** that participants will examine risk factors for victimization, discuss available resources for prevention and recovery, and approach these issues through a case management lens to identify best practices for supporting older adults and other victims with dignity, autonomy, and resilience.

**Acknowledge** that participants may come to this training with different levels of experience in APS investigations and service planning. Some may have extensive experience with fraud cases, while others may be newer to the field. This training begins with foundational knowledge of fraud dynamics and the aging brain to ensure a shared understanding before moving into service planning strategies.

## Slide #8: Introduction to “Fraud” and “Scams”



**Share** that we are all regularly exposed to scams via various online platforms every day. Some come:

- Via text or phone calls
- Through social media and email.

**Reinforce** the following language use guidance for this training:

- “Scam” is a term without necessary legal meaning and is synonymous with fraud.
- “Fraud” is the more appropriate term as it’s largely defined in both academic studies and legal systems as a behavior where an individual uses deception (lying, misrepresenting themselves) to trick victims into providing them with money, personal information, property, or other resources they control.
- There are laws in all 50 states and the federal government related to fraud, whether in person or online.
  - Using the term fraud helps individuals to understand that they have been victimized and can get assistance from governmental and non-profit agencies.

**Explain** that:

- Both “scam” and “fraud” may be used informally and interchangeably in this training.
- Participants can be mindful of context, using “fraud” in documentation, legal reporting, and professional communication, while recognizing that “scam” may be more accessible in everyday conversation.
- This flexibility supports clearer communication with clients, colleagues, and community partners.

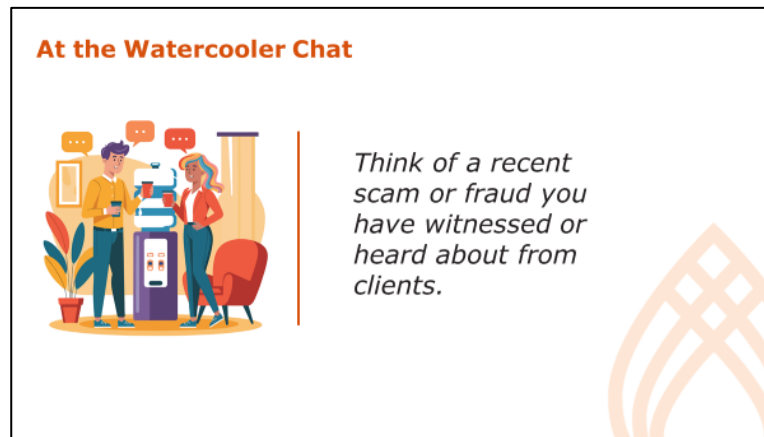
**Ask** participants to reflect on the language used to describe individuals who have experienced scams or fraud.

**Clarify** the distinction for the purpose of this training:

- “Victim” is appropriate in legal, investigative, and reporting contexts. It clearly communicates that a crime occurred and that the person was harmed.
- “Survivor” is often used in recovery and support contexts. It emphasizes resilience.

**Share** that in this training, we honor the agency of our clients and respect how they interpret their experience. Whether someone prefers the term “victim,” “survivor,” or another descriptor, APS professionals should follow the client’s lead and use language that affirms their experience.

## Slide #9: At the Watercooler Scams Chat



### **Activity: At the Watercooler (5-10 minutes)**

#### ***Small Breakout Groups***

**Explain** that scams and fraud are not just abstract risks, they're experiences that affect people across all walks of life, including APS professionals and the clients they serve. This activity invites participants to engage in informal "watercooler-style" conversations, surfacing real-world examples and building connection through shared stories. These conversations help normalize the experience of encountering scams and highlight the emotional and contextual complexity behind each case.

#### **Instructions:**

- **Ask** participants to spend a few moments thinking of a recent scam or fraud experience they've encountered or heard about from clients.
- **Explain** to participants that they will be broken into small groups of three (3) to spend a few minutes at the virtual water cooler exchanging stories of scam/fraud schemes.
- **Ensure** participants understand the importance of confidentiality and avoiding personally identifying information.
- **Gather** participants back into the large group.
- **Ask** participants to type into the chat a response to the following question: "What did your group's discussion reveal about how complex scams can be?"

#### **Trainer note:**

- *Use responses to highlight the diversity of scam tactics and emotional responses.*
- *Reinforce that scams are not just financial, they're psychological, social, and often traumatic.*

- *Emphasize that addressing scams in APS casework requires nuanced, person-directed approaches.*
- *Transition into the next section by noting that the complexity of scams mirrors the complexity of interventions APS professionals must consider.*

## Types and Impact of Fraud

**Time Allotted:** 75 minutes

**Associated Objective(s):** Recognize prevalent types of scams impacting the APS client population and the role of technology and social engineering used.

**Method:** Instruction, Discussion, Word Clouds, Small Groups, Resource Mapping

## Slide #10: Fraud and Manipulation

**Fraud and Manipulation**

**SOCIAL ENGINEERING**

Manipulating people into giving up information or access

- If you see someone in a brown uniform carrying a box, what do you assume?
- If your boss usually emails you during work hours, how would you react to a midnight message?
- When you get a friend or an email from your bank, how closely do you check the sender's details?

*Trainer note: this slide is animated.*

**Share** that it is critical to understand that fraud is a problem that affects anyone because of the ways in which fraudsters present themselves.

- Most forms of online fraud involve the use of tactics referred to as “social engineering,” which refers to misrepresenting oneself in order to gain something of value from a target of a scam or fraud.
- This term comes from computer hacking, reflecting on the obvious vulnerabilities and flaws in the human psyche that lead us to give away information or resources to those we perceive as trustworthy or in need of aid.

### **Activity: Everyday Assumptions, Everyday Risks (5-10 minutes)**

#### ***Individual Reflection, Large Group Virtual Chat Discussion***

**Introduce** the activity by explaining that scammers often rely on our automatic assumptions and mental shortcuts, known as cognitive biases, to manipulate us. These biases help us navigate the world efficiently, but they can also make us vulnerable to deception.

#### **Instructions:**

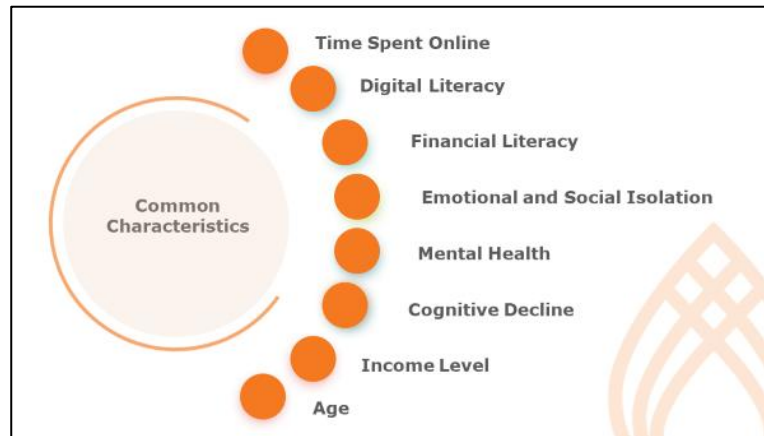
- **Ask** participants to reflect individually on how they respond to common situations. Use prompts such as:
  - “If you see someone in a brown uniform carrying a box, what do you assume?”
  - “If your boss usually emails you during work hours, how would you react to a midnight message?”

- "When you get a friend request or an email from your bank, how closely do you check the sender's details?"
- **Invite** participants to type their responses into the chat box.
- **Facilitate** a brief discussion by highlighting patterns in the responses and connecting them to scam tactics.
- **Reinforce** that these assumptions are normal and not signs of gullibility, they are human tendencies that fraudsters exploit.
- **Transition** by emphasizing that understanding these patterns helps APS professionals communicate with clients in a nonjudgmental, trauma-informed way.

*Trainer note: Use this activity to normalize the experience of being manipulated and reduce stigma. Encourage participants to reflect on how these biases may show up in their own casework or personal lives. This activity sets the stage for deeper exploration of fraud types and victim impacts.*



## Slide #11: Common Risk Factors for Fraud Victimization



**Share** that fraud is such a prominent part of the online experience in modern society. Older adults, as more than 75% report using the Internet every day according to the Pew Charitable Trust. This is in stark contrast to the early 2000s, when 14% of older people were online.

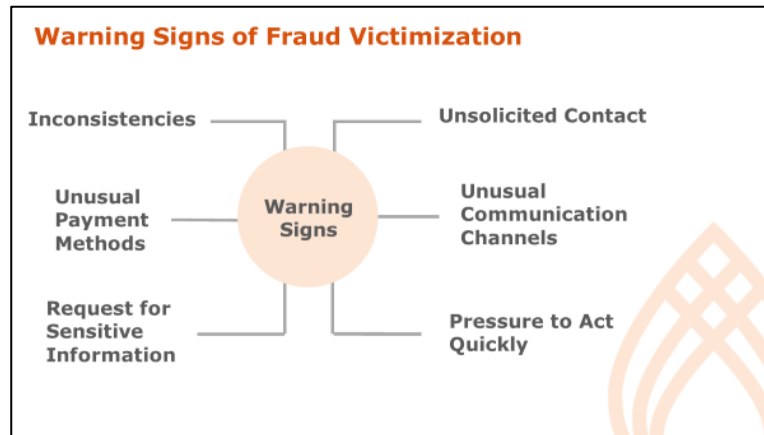
**Review** the following highlighted risk factors associated with fraud risk:

- Time Spent Online
  - Frequent use of social media or online shopping increases exposure to scams.
  - Individuals expecting deliveries may be more susceptible to phishing or smishing scams.
- Digital Literacy
  - Limited understanding of how banks or retailers communicate can lead to misinterpreting fraudulent messages as legitimate.
  - New users may not recognize red flags in friend requests or online interactions.
- Financial Literacy
  - Lack of understanding of payment systems (e.g., wire transfers, crypto) can increase vulnerability.
- Isolation
  - Loneliness can lead individuals to engage with strangers online, increasing susceptibility to romance or friendship scams.
- Mental Health
  - Experiencing mental health symptoms like depression and anxiety makes individuals more vulnerable to exploitation.

- People experiencing mental health issues were 5-10 times more likely to be financially exploited (DeMarco, 2025).
- Cognitive Decline
  - Individuals with memory or processing challenges may struggle to assess the legitimacy of requests or communications.
  - This will be explored further in the Neurocognitive Ability and Susceptibility Factors section.
- Income Level
  - Higher-income individuals may be targeted for investment scams.
  - Lower-income individuals may experience more severe consequences from smaller losses.
- Age
  - Fraud affects all age groups. Middle-aged adults report the highest rates, but older adults may face more severe impacts due to isolation or cognitive decline.

*Trainer note: Encourage participants to reflect on which of these risk factors they've observed in their own casework. Consider prompting a brief chat or verbal share-out to connect the content to real-world APS experiences.*

## Slide #12: Warning Signs of Fraud Victimization



**Share** that while scams vary in tactics, there are consistent red flags that show up across many types of fraud. Recognizing these patterns helps APS professionals identify risk and respond effectively, especially when clients may not realize they've been targeted.

**Review** the following universal red flags:

- Unsolicited contact from unknown individuals or organizations
- Requests for sensitive information (e.g., SSN, bank details, login credentials)
- Pressure to act quickly or secrecy (e.g., "Don't tell anyone")
- Requests for payment via gift cards, wire transfers, or cryptocurrency
- Unusual communication channels (e.g., social media, messaging apps)
- Emotional manipulation (e.g., urgency, fear, affection)
- Inconsistencies in story or identity

**Explain** that these red flags often show up in APS casework as vague or confusing client reports. Clients may describe feeling pressured, scared, or emotionally invested without realizing they've been defrauded.

*Trainer note: Use this slide to transition into scam-specific examples. Encourage participants to reflect on how these red flags show up in their own casework and how they can use pattern recognition to support clients. You may also ask participants to share examples they've encountered and match them to the red flags listed.*

## Slide #13: Fraud Types: Phone Scams – How They Work



**Explain** that phone scams, often referred to as “call center scams,” remain one of the most common and damaging forms of fraud targeting older adults. These scams are particularly effective because they exploit trust, urgency, and confusion, often using official-sounding language and personal information obtained through data breaches or public records.

**Discuss** the following key points:

- These scams usually begin with an unsolicited phone call. The caller may already know the victim’s name, address, or other personal details, which makes the interaction feel legitimate. The scammer then presents a fabricated situation that requires immediate action—often involving money, personal information, or access to the victim’s computer.
- Common phone scam variants:
  - Government impersonation scams: The caller claims to be from the IRS, Social Security Administration, or another government agency, demanding payment for a supposed debt or threatening legal action.
  - Charity scams: The scammer pretends to represent a charitable organization, often following a natural disaster or crisis, and pressures the victim to donate.
  - Tech support scams: The caller claims to be from a tech company, warning that the victim’s computer is “infected.” They then instruct the victim to download software that gives the scammer remote access to the device, often leading to identity theft or financial loss.
- Many older adults still rely on landlines and may be more likely to answer unknown calls. They may also be more trusting of authority figures or less familiar with the tactics used in modern fraud schemes. Cognitive changes,

hearing loss, or social isolation can further increase vulnerability, which will be explored together in further detail in this training.

## Slide #14: Fraud Types: Phone Scams – Red Flags

**Fraud Type: Phone Scams – Red Flags**



- High-pressure tactics or threats
- Requests for gift cards or wire transfer
- Instructions to download software
- Refusal to provide verifiable contact info
- Caller claims urgency or secrecy

**Discuss** the following APS casework clues for phone scams:

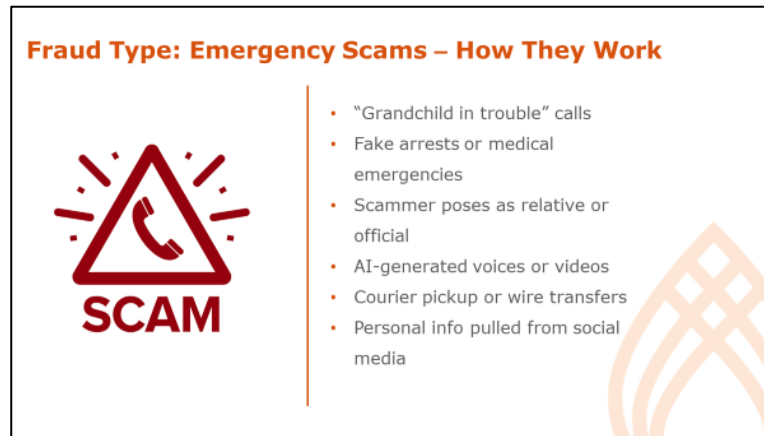
- Clients may say things like:
  - “Someone from the IRS called and said I owed money.”
  - “They told me my computer had a virus and I needed to act fast.”
  - “I didn’t want to get in trouble, so I followed their instructions.”

**Highlight** the following red flags:

Red Flags	Scam Connection
High-pressure tactics or threats	Government impersonation
Requests for gift cards or wire transfers	Payment red flag
Instructions to download software	Tech support scam
Refusal to provide verifiable contact info	Avoids traceability
Caller claims urgency or secrecy	Emotional manipulation tactics

***Trainer note:** Encourage participants to reflect on how these scams may show up in their casework. Ask them to consider how clients might describe these experiences, often not as “fraud,” but as a confusing or upsetting phone call. Reinforce the importance of listening for clues, validating the client’s experience, and gently exploring whether a scam may have occurred.*

## Slide #15: Fraud Types: Emergency Scams – How They Work



**Explain** that emergency scams, sometimes called "grandparent scams" or "crisis scams," are emotionally manipulative schemes that exploit a victim's instinct to protect loved ones. These scams are increasingly sophisticated, often using artificial intelligence (AI) to mimic voices or create convincing messages that appear to come from a family member in distress. These scams are increasingly sophisticated and often use urgency, secrecy, and emotional pressure to override logical thinking.

**Discuss** the following key points:

- The scam typically begins with a phone call, text, or social media message claiming that a loved one, often a grandchild, niece/nephew, or children are in urgent trouble. The caller may say they've been arrested, hospitalized, or stranded in a foreign country and need immediate financial help. The scammer may pose as the relative or as a police officer, lawyer, or medical professional speaking on their behalf.
- Scammers can now generate realistic voice clones or video messages using publicly available content (e.g., social media posts, YouTube videos). This makes the scam feel more authentic and emotionally compelling. Victims may hear what sounds like their loved one crying or pleading for help, which can override logical thinking and increase compliance.
- Scammers often pressure the victim to act immediately before they can verify the story. They may say, "Don't tell anyone," or "You'll make things worse if you delay." This urgency is designed to prevent the victim from checking with family members or thinking critically about the situation.

- Victims are typically asked to send money via wire transfer, gift cards, or cryptocurrency. In some cases, scammers may even send a courier to pick up cash in person.
- Scammers may gather personal details from hacked or public social media accounts to make their story more believable. They might reference real names, locations, or events to build trust and credibility.



## Slide #16: Fraud Types: Emergency Scams – Red Flags

**Fraud Type: Emergency Scams – Red Flags**



- Urgency and secrecy
- Emotional manipulation
- Gift cards or wire transfer requests
- AI-generated voice or video
- "Don't tell anyone"

**Discuss** the following APS casework clues for emergency scams:

- Clients may say things like:
  - "I got a call from my grandson, he was crying and needed bail money."
  - "They told me not to tell anyone or it would make things worse."
  - "I sent gift cards because they said it was the fastest way to help."

**Highlight** the following red flags:

Red Flag	Scam Connection
Urgency and secrecy	Emergency scam tactic
Emotional manipulation	Exploits protective instincts
Gift card or wire transfer request	Payment method red flag
AI-generated voice or video	Deepfake deception
"Don't tell anyone"	Isolation tactic

*Trainer note: Reinforce that APS professionals should be alert to signs that a client has been manipulated through fear or urgency. If a client mentions sending money to help a relative in trouble, especially if they were told not to tell anyone, this may indicate an emergency scam. Validate the client's emotional response and gently explore the details of the situation. Encourage clients to verify any emergency claims through a trusted contact or by calling the person directly using a known number.*

## Slide #17: Fraud Types: Phishing/Smishing – How They Work

**Fraud Type: Phishing/Smishing – How They Work**



- Phishing = fake emails
- Smishing = fake texts
- Impersonate banks or agencies
- Urgent messages trigger fear
- Fake links steal info
- Realistic websites mimic legit ones
- May include partial personal info
- Targets email & smartphone users

**Explain** that phishing and smishing scams are among the most widespread and evolving forms of fraud. These schemes rely on deception and urgency to trick individuals into revealing sensitive information or clicking malicious links. They are especially dangerous because they often appear to come from trusted sources and can be difficult to detect, particularly for clients with limited digital literacy.

**Discuss** the following key points:

- Phishing is a form of online fraud where scammers send emails that appear to come from legitimate organizations, such as banks, government agencies, or popular online streaming services or delivery services. These emails often contain urgent messages (e.g., "Your account has been compromised!") and include links to fake websites designed to steal login credentials, credit card numbers, or other personal information.
- Smishing is the text message version of phishing. These scams arrive via SMS or messaging apps and often impersonate delivery services (e.g., mail delivery services), financial institutions, or government agencies. The message typically includes a link or phone number and urges the recipient to act quickly, such as confirming a package, verifying account details, or resolving a supposed legal issue.
- These messages are designed to trigger emotional responses like fear, urgency, or curiosity, before the recipient has time to think critically. The links often lead to websites that look nearly identical to real ones, making it easy to fall for the scam. Some messages may even include partial personal information (e.g., name or last four digits of an account) to increase credibility.

- Common red flags:
  - Unexpected messages from banks, government agencies, or service providers
  - Spelling or grammar errors in the message
  - Requests for personal or financial information
  - Links that don't match the official website URL
  - Pressure to act immediately or face consequences
- While phishing primarily targets email users, smishing affects anyone with a smartphone, especially those using iPhones or Android devices. Older adults may be more vulnerable if they are unfamiliar with how legitimate institutions communicate or if they rely heavily on text-based communication.

## Slide #18: Fraud Types: Phishing/Smishing – Red Flags

**Fraud Type: Phishing/Smishing – Red Flags**



- Unexpected messages from banks or agencies
- Spelling or grammar errors
- Requests for personal or financial info
- Links that don't match official URLs
- Pressure to act immediately
- Mention of compromised accounts or packages

**Discuss** the following APS casework clues. Clients may say things like:

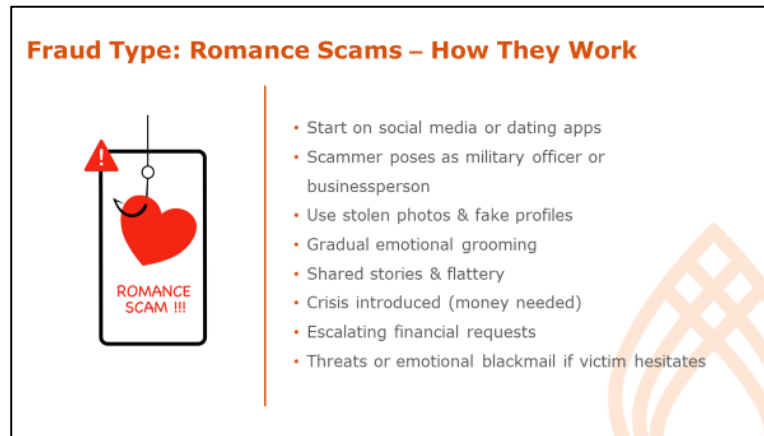
- “I got a text saying my bank account was locked and I needed to click a link.”
- “I received an email from Netflix saying my payment failed, but I don’t even have an account.”
- “I clicked a link to track a package, and now my phone is acting weird.”
- “They asked me to confirm my Social Security number to avoid legal trouble.”

**Highlight** the following red flags:

Red Flag	Scam Connection
Unexpected messages from banks or agencies	Impersonation via email or text
Spelling or grammar errors	Common in scam messages
Requests for personal or financial info	Identity theft or account takeover
Links that don’t match official URLs	Redirects to fake websites
Pressure to act immediately	Emotional manipulation tactic
Mention of compromised accounts or packages	Common phishing/smishing bait

**Encourage** participants to listen for clues in client conversations—such as mentions of suspicious texts, emails, or account issues. Clients may not use the term “phishing” or “smishing,” but they may describe feeling confused, pressured, or tricked into clicking a link or sharing information.

## Slide #19: Fraud Types: Romance Scams – How They Work



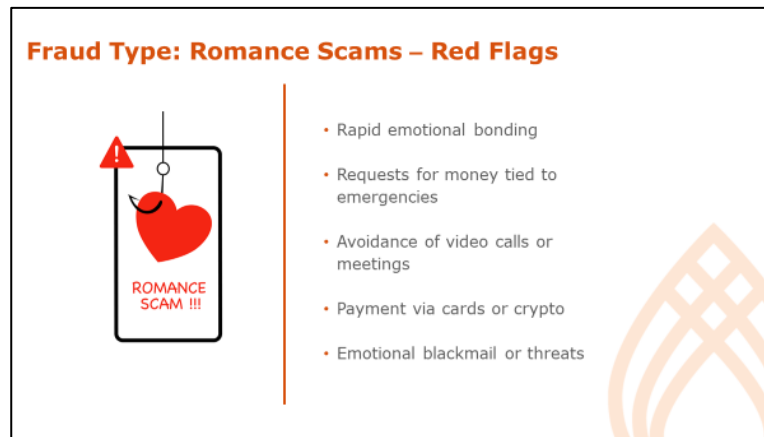
**Explain** that romance fraud is one of the most emotionally devastating forms of financial exploitation. These scams are designed to build trust and emotional attachment before exploiting the victim financially, often over weeks or months. The emotional manipulation involved can lead to deep shame, grief, and long-term trauma, making it especially difficult for victims to come forward or accept help.

**Discuss** the following key points:

- Romance scams typically start on social media platforms, dating apps, or through unsolicited messages. The scammer may pose as a widowed military officer, a businessperson working overseas, or someone seeking companionship. They often use stolen photos and fabricated profiles to appear trustworthy and relatable.
- Romance scammers often engage in a process similar to grooming, or gradually building trust and emotional dependency through flattery, shared stories, and expressions of affection. This manipulation is intentional and strategic, designed to lower the victim's defenses and create a sense of intimacy. The scammer may mirror the victim's interests, offer emotional support, and ask for personal details or photos to deepen the connection. Over time, this emotional bond can override logic and make the victim more susceptible to financial exploitation.
- Once trust is established, the scammer introduces a crisis: they need money for a plane ticket, medical emergency, legal trouble, or to help a family member. These requests often escalate over time. If the victim complies, the scammer continues to invent new emergencies to extract more money.

- If the victim hesitates or runs out of money, the scammer may become manipulative or threatening. They might use guilt, emotional blackmail, or even threaten to release private photos or messages. This can create a cycle of fear and compliance, especially if the victim is isolated or emotionally invested.
- Scammers often request funds through hard-to-trace methods such as:
  - Cryptocurrency
  - Gift cards
  - Wire transfers or prepaid debit cards
  - If a client is purchasing gift cards in unusual quantities or asking about cryptocurrency, this may be a red flag.
- Victims of romance fraud often experience what researchers call “double victimization,” the loss of both money and a perceived relationship. The emotional fallout can include grief, shame, depression, and social withdrawal. Many victims are reluctant to report the fraud due to embarrassment or fear of being judged.

## Slide #20: Fraud Types: Romance Scams – Red Flags



**Discuss** the following APS casework clues for romance scams:

- Clients may say things like:
  - “I’ve been talking to someone online who really understands me.”
  - “They’re overseas and need help with a plane ticket or medical bills.”
  - “We haven’t met in person, but I feel like we’re in love.”
  - “They asked me to send gift cards or cryptocurrency to help their situation.”
- These statements often reflect emotional investment and trust, even when the relationship is entirely virtual. Clients may not recognize the situation as fraud, especially if they’re still emotionally attached.

**Highlight** the following red flags:

Red Flag	Scam Connection
Rapid emotional bonding	Grooming and manipulation tactic
Requests for money tied to emergencies	Escalating financial exploitation
Avoidance of video calls or meetings	Identity concealment
Payment via gift cards or crypto	Hard-to-trace methods favored by scammers
Emotional blackmail or threats	Coercion when victim hesitates
Shame or secrecy around relationship	Isolation and control tactic



**Encourage** participants to approach these cases with empathy and without judgment. Clients may not recognize that they've been defrauded, especially if they still believe the relationship is real.

## Slide #21: Fraud Types: Investment Fraud – How They Work



**Explain** that investment fraud, particularly involving cryptocurrency, is one of the fastest-growing and most financially devastating scams affecting older adults. These schemes often appear sophisticated and legitimate, and they prey on a person’s desire for financial security, independence, or even connection. In many cases, they are intertwined with romance scams or other forms of emotional manipulation.

**Discuss** the following key points:

- These scams often start with unsolicited contact through social media, dating apps, or messaging platforms. The scammer may first build rapport, sometimes through a romantic pretext, and then introduce the idea of a “lucrative investment opportunity.” They may claim to have insider knowledge or access to a new cryptocurrency or trading platform.
- Victims are directed to professional-looking websites or apps that simulate real-time investment dashboards. These platforms show fake gains, encouraging the victim to invest more money. The scammer may pose as a financial advisor or connect the victim with a so-called “investment team,” who are part of the fraud network.
- As the victim sees their “investment” grow, they are encouraged to deposit more funds to maximize returns. When they attempt to withdraw money, they are told they must first pay taxes, fees, or penalties. These demands continue until the victim either runs out of money or realizes they’ve been defrauded.
- Common Payment Methods:

- Cryptocurrency, which is difficult to trace and nearly impossible to recover
  - Wire transfers or prepaid debit cards
  - Gift cards in smaller denominations, which may seem less suspicious
  - If a client is asking about cryptocurrency, purchasing gift cards in unusual amounts, or referencing an online investment opportunity, these may be red flags.
- These scams often exploit hope, fear, and trust. Victims may feel excited about the possibility of financial independence or helping their family. Once defrauded, they may feel ashamed, confused, or reluctant to disclose what happened, especially if they were warned by others and ignored the advice.
- Investment fraud can lead to catastrophic financial losses, especially for clients on fixed incomes or those managing chronic health conditions. It may also signal cognitive decline if the client is unable to recognize red flags or continues to engage with the scam despite evidence of fraud.

## Slide #22: Fraud Types: Investment Fraud – Red Flags

**Fraud Type: Investment Fraud – Red Flags**



- Unsolicited investment advice
- Guaranteed high returns
- Fake dashboards showing growth
- Request for crypto, wire, or gift cards
- "Pay fees/taxes to withdraw"
- Emotional manipulation or secrecy

**Discuss** the following APS casework clues:

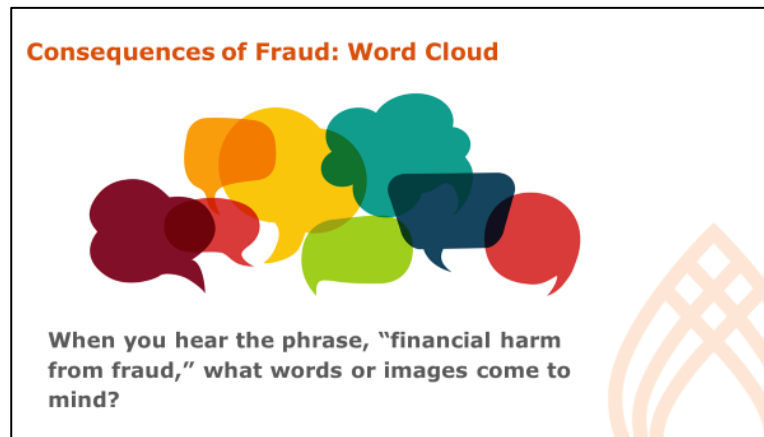
- Clients may say things like:
  - "I met someone online who told me about a great investment opportunity."
  - "I saw my money growing on the app, but now I can't withdraw it."
  - "They said I had to pay taxes or fees before I could get my earnings."
  - "I didn't want to miss out, so I sent more money."
- These statements often reflect hope, urgency, and trust, and clients may still believe the investment is real, even after significant losses.

**Highlight** the following red flags:

Red Flags	Scam Connection
Unsolicited investment advice	Often begins via social media or dating apps
"Guaranteed" high returns	Classic hallmark of fraudulent investments
Fake dashboards showing growth	Illusion of legitimacy to encourage deposits
Requests for crypto, wire, or gift cards	Hard-to-trace payment methods
"Pay fees/taxes to withdraw"	Escalating financial manipulation
Emotional manipulation or secrecy	Often overlaps with romance or affinity scams

**Encourage** participants to approach these cases with empathy and curiosity. Clients may still believe the investment is real or maybe too embarrassed to admit they were misled. Use open-ended questions to explore the situation and assess risk. Consider involving trusted supports, financial institutions, or legal services when appropriate. Reinforce that anyone can be targeted—and that recovery begins with support, not shame.

## Slide #23: Consequences of Fraud: Word Cloud



### **Activity: Financial Harm Word Cloud (5 minutes)**

#### ***Word Cloud***

#### **Instructions:**

- **Ask** participants, "when you hear the phrase 'financial harm from fraud,' what words or images come to mind?"
- **Launch** a word cloud tool (e.g., Mentimeter, Poll Everywhere) or use the chat box to collect responses.
- **Debrief** by highlighting common themes (e.g., loss, shame, instability, fear) and connecting them to APS casework.
- **Reinforce** that financial harm is not just about the dollar amount lost, it can have cascading effects on a client's housing, health, and emotional well-being.
- **Encourage** participants to consider how financial harm intersects with other risk factors discussed earlier (e.g., cognitive decline, isolation, income level).

Following the activity, **share** that financial harm is often the most visible and immediate consequence of fraud victimization. This section explores the direct and indirect financial impacts, including identity theft, loss of savings, and the cost of recovery.

## Slide #24: Consequences of Fraud: Financial Harm



**Discuss** the following possible financial harms:

- Most fraud schemes involve the transfer of money or assets under false pretenses.
- Losses can range from small amounts to life savings, depending on the type of scam and the client's financial situation.
- According to the FBI's Internet Crime Complaint Center (IC3), older adults reported over \$3.4 billion in losses due to fraud in 2023, with investment scams and tech support scams among the costliest.
- Many scams involve the theft of personal information (e.g., Social Security numbers, bank credentials, Medicare IDs).
- This can lead to unauthorized charges, new accounts opened in the victim's name, or fraudulent use of medical benefits.
- Victims may not be aware of the full extent of the harm until months later.
- Victims often incur additional expenses trying to recover from fraud:
  - Replacing stolen IDs or insurance cards
  - Paying for credit monitoring or legal assistance
  - Covering overdraft fees or penalties from fraudulent transactions
- These costs can be especially burdensome for clients on fixed incomes or with limited financial literacy.
- Financial harm can disrupt a client's ability to pay rent, purchase medication, or maintain utilities.
- APS professionals may need to coordinate emergency financial assistance, connect clients with fiduciary services, or explore protective interventions (e.g., representative payee, POA).

## Slide #25: Consequences of Fraud: Emotional Harm



**Waterfall Chat**

### Consequences of Fraud: Emotional Harm

- Shame, embarrassment shaped by others' reactions
- Ageism can worsen emotional harm
- Fear of losing financial control
- Worry about being judged or deemed incapable
- Social withdrawal, isolation, increased vulnerability
- Anxiety, depression, PTSD symptoms

*Trainer note: this slide is animated.*

### **Activity: Emotional Impact Reflection (5 minutes)**

#### **Waterfall Chat**

#### **Instructions:**

- **Explain** the waterfall chat method:
  - Participants should type their responses into the chat box but do not press enter yet.
  - Let them know you'll give a signal when everyone should press enter at the same time.
- **Ask** participants: "When someone experiences fraud, what emotions do you think they might feel, both immediately and over time?"
- **Give** participants 30–60 seconds to reflect and type their responses.
- **Say:** "Okay, press enter now!" to release all responses simultaneously.
- **Observe** the chat and highlight common emotional themes.

**Debrief** the activity by highlighting common emotional responses such as shame, fear, grief, anger, betrayal, and confusion. Many experience intense shame, believing they "should have known better," which can prevent them from seeking help. This is especially true for older adults, who may fear being seen as incompetent or losing their independence.

**Discuss** the following key points:

- Clients may feel a sense of shame or embarrassment when they realize they were manipulated in a scam. This reaction is often shaped by how others respond, especially if the situation is seen as something they should have recognized. These feelings can be compounded by ageist assumptions that older adults are less capable or less familiar with technology. It is



important to affirm that anyone can be impacted and that scammers use highly sophisticated tactics designed to exploit trust, emotion, and urgency.

- Older adults may fear that disclosing the fraud will lead to loss of control over their finances or living situation. They may worry that family members or professionals will question their cognitive abilities or decision-making capacity.
- Emotional harm can lead to social withdrawal, especially if the victim feels embarrassed or fears being blamed. This isolation can increase vulnerability to future scams and worsen mental health outcomes.
- Research shows that fraud victimization can lead to symptoms of anxiety, depression, and even post-traumatic stress. According to Maher & Hayes (2024), victims who suffer financial loss are significantly more likely to report emotional distress and behavioral health challenges.

**Encourage** participants to reflect on how emotional harm may show up in their clients. For example, through changes in mood, reluctance to talk about finances, or avoidance of social contact. **Emphasize** that validating the client's experience and using nonjudgmental language is essential to building trust and supporting recovery.

## Slide #26: Consequences of Fraud Victimization: Health and Social



**Explain** that health and social consequences often emerge gradually and may not be immediately visible. **Encourage** participants to consider how these impacts may show up in their clients' lives and how they intersect with other risk factors such as cognitive decline, isolation, and chronic illness.

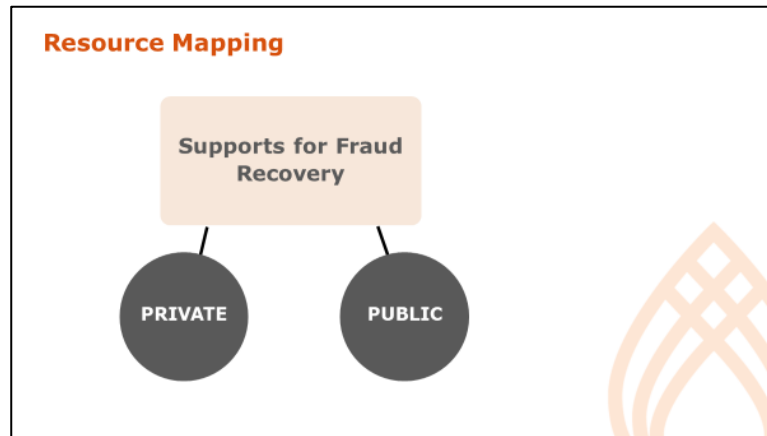
**Discuss** the following key points:

- The stress of losing money, especially funds needed for rent, medication, or food, can lead to a cascade of physical symptoms. Victims may experience insomnia, headaches, gastrointestinal issues, elevated blood pressure, or exacerbation of chronic conditions. Prolonged stress can also suppress immune function and increase the risk of cardiovascular events.
- Victims may develop anxiety, depression, or symptoms of post-traumatic stress. These conditions can be triggered by the trauma of being deceived, the fear of future victimization, or the shame of disclosing what happened. For some, the emotional toll may lead to suicidal ideation, particularly if the financial loss was severe or if they feel unsupported.
- Many victims withdraw from family, friends, or community activities due to embarrassment or fear of judgment. This isolation can deepen emotional distress and increase vulnerability to future scams. In some cases, victims may avoid using technology altogether, cutting off important sources of connection and support.
- Older adults may fear that disclosing the fraud will result in loss of autonomy, such as being placed under financial oversight or losing control of their living situation. This fear can prevent them from seeking help and may lead to further harm.

- Victims may struggle to manage daily tasks due to emotional distress or the practical fallout of fraud (e.g., closing bank accounts, replacing IDs, dealing with creditors). These disruptions can interfere with medication adherence, nutrition, and access to care.

**Reinforce** that APS professionals should assess both visible and hidden impacts of fraud. Ask about changes in sleep, appetite, mood, or social engagement.

## Slide #27: Resource Mapping



### **Activity: Identifying Public and Private Supports for Fraud Recovery (15 minutes)**

#### ***Small Group Work***

**Explain** that this activity helps participants identify and differentiate between public and private sector resources available to support clients who have experienced fraud. It reinforces earlier content on the consequences of fraud and prepares participants for person-directed service planning by expanding their awareness of referral options.

#### **Instructions:**

- **Divide** participants into groups of three to four participants and assign groups as either Public Sector Resources or Private Sector Resources:
- **Tell** participants that each group will have 10 minutes to brainstorm and list as many relevant resources as possible that could support a client who has experienced fraud. **Instruct** them to take note of these resources on the **Handout: Fraud Recovery Resource Mapping Worksheet**.
- **Encourage** them to think broadly and consider:
  - Prevention
  - Reporting
  - Emotional support
  - Financial recovery
  - Legal advocacy
  - Technology assistance

- **Remind** participants that not all agencies will take action in every case. For example, local police may not investigate if the scammer is overseas, but filing a report is still important for documentation and validation.
- **Encourage** participants to think about **local** resources they've used or referred to in their own counties or regions.
- **Bring** everyone back to the main room. **Ask** participants to share one of the resources they plan to use for future cases addressing fraud against their clients.
- **Facilitate** a brief discussion using the following questions:
  - Were there any resources that surprised you?
  - How do you decide which resource to refer a client to first?
- **Review** Key Takeaways:
  - Fraud recovery often requires a multi-system response.
  - Knowing the limitations and strengths of each resource helps tailor referrals to the client's needs and preferences.
  - Building a local resource list is essential for effective, person-directed service planning.
- **Direct** participants to the **Resource Handout** in the **Appendix** after the activity to compare and expand their lists.

## Handout: Fraud Recovery Resource Mapping Worksheet

Resource Name and Contact Information	Type of Resource	Public or Private	Notes

## Neurocognitive Ability and Susceptibility Factors


**Time Allotted:** 45 minutes

**Associated Objective(s):** Describe the psychological, cognitive, and social factors that increase scam susceptibility and barriers to reporting.

**Method:** Lecture, Poll, Large Group Discussion

## Slide #28: Correlation Between Fraud and the Brain

**Correlation Between Fraud and the Brain**



- Age-related changes affect risk detection and decision-making
- Emotional scams bypass logic targeting reward and attachment systems

**Share** that this section marks a shift from identifying external fraud tactics to exploring internal vulnerabilities, specifically, how age-related and other conditions impacting brain function can influence decision-making and increase susceptibility to scams. It builds on the emotional and psychological impacts discussed earlier and introduces a neurobiological lens to deepen understanding.

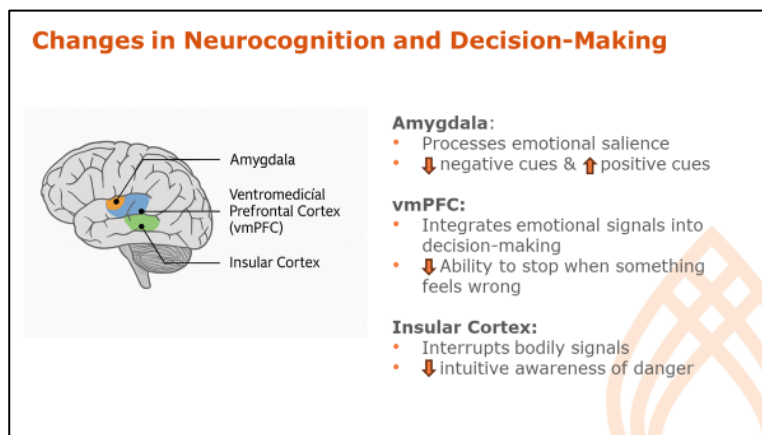
- Recognize that vulnerability to fraud is not simply about unsafe choices or lack of awareness.
- Understand how scammers exploit emotional and cognitive processes.
- Begin thinking about how neurological changes may affect client behavior, risk perception, and response to interventions.

**Share** that fraud victimization is not just a financial issue, it's a deeply emotional experience. It's essential to understand that decision-making difficulties in older adults are not always due to neurocognitive disorders.

- Many scams, particularly romance scams, are designed to exploit the brain's emotional systems, bypassing logical reasoning and activating neural circuits tied to reward, attachment, and trust.
- This manipulation is especially dangerous for older adults who have age-related changes in brain function, particularly in regions like the amygdala and ventromedial prefrontal cortex. These changes can impair their ability to detect risk, regulate emotion, and resist emotionally charged appeals.
- The same can be true for others who are also experiencing adverse neurocognitive impacts due to medical conditions and/or injuries to specific areas of the brain.



## Slide #29: Changes in Neurocognition and Decision-Making



**Explain** that while our brains have multiple functions, this section will discuss three areas of the brain as they relate to scam susceptibility.

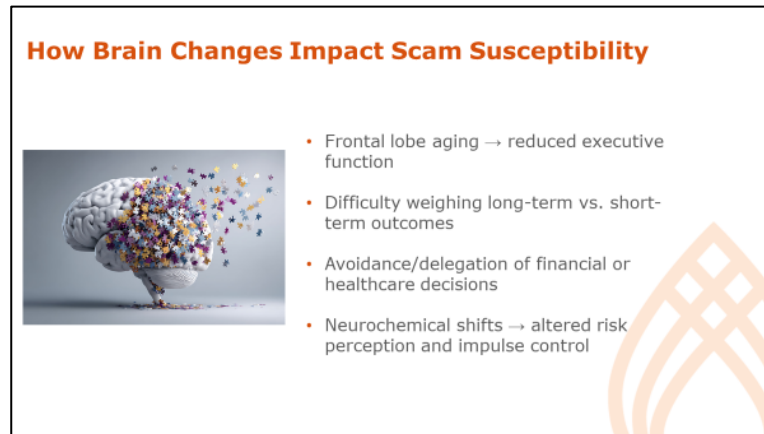
**Review** the key brain regions involved:

- **Amygdala:** Processes emotional salience, especially fear, trust, and reward. In aging, the amygdala may become less responsive to negative cues (e.g., risk, deception) and more responsive to positive cues (e.g., affection, attention).
- **Ventromedial Prefrontal Cortex (vmPFC):** Integrates emotional signals into decision-making. Age-related decline in this region can impair the brain's ability to send a "stop" signal when something feels wrong.
- **Insular Cortex:** Interprets bodily signals (e.g., gut feelings). Deterioration here can reduce intuitive awareness of danger.

**Review** What This Means for APS Clients:

- Adults who have changes in the above regions of the brain may feel emotionally connected to a fraudster and trust them, even when the facts suggest otherwise.
- The "emotional override" effect: When the vmPFC and amygdala are impaired, people rely more on emotions than logic to make decisions.
- Scammers exploit this by creating urgency, affection, or fear, triggering emotional responses that short-circuit rational thinking.
- In romance scams, the emotional bond can be so strong that the brain's internal "stop" signal, normally triggered by risk or doubt, fails to activate.

## Slide #30: How Brain Changes Impact Scam Susceptibility

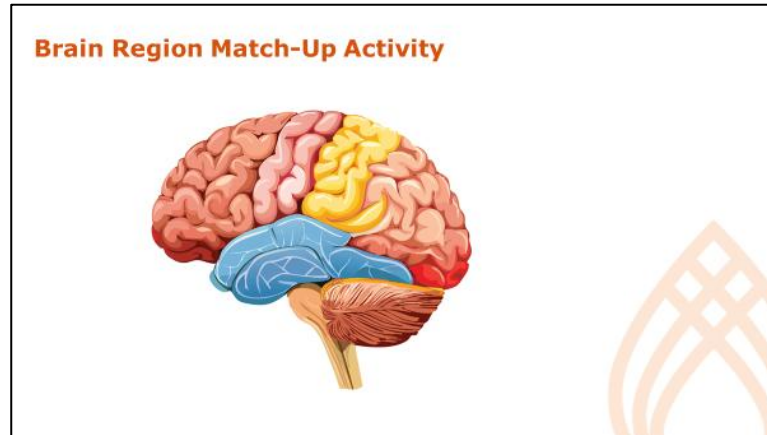


### **Discuss** additional key points:

- Frontal lobe aging can reduce executive function, making it harder to weigh long-term consequences vs. short term benefits.
- Older adults may avoid or delegate difficult decisions, especially around finances or healthcare, increasing vulnerability.
- Neurochemical changes (e.g., dopamine, serotonin) can alter risk perception and impulse control.
  - Risk Perception: Lower dopamine levels can reduce the brain's ability to evaluate risk and reward. An older adult might not recognize a scam as dangerous or may underestimate the consequences.
  - Impulse Control: Changes in serotonin can make it harder to pause and reflect before acting. This might lead to impulsive decisions — like sending money quickly or clicking on a suspicious link, without fully processing the situation.
  - Medications that impact serotonin and dopamine levels should be evaluated if the person taking the medication is being scammed or defrauded.

**Encourage** participants to reflect on how these neurological changes might show up in their own casework. Clients may appear “irrational” or “in denial,” but these behaviors may be rooted in real cognitive shifts. Remembering how these neurological changes impact people's behaviors can allow you to be compassionate and understanding of why people maybe making unsafe decisions when you interview them.

## Slide #31: Brain Region Match-Up



### **Activity: Brain Region Match-Up (5-7 minutes)**

#### ***Polling***

**Inform** participants know they'll be doing a quick knowledge check to reinforce key brain regions and their role in scam susceptibility.

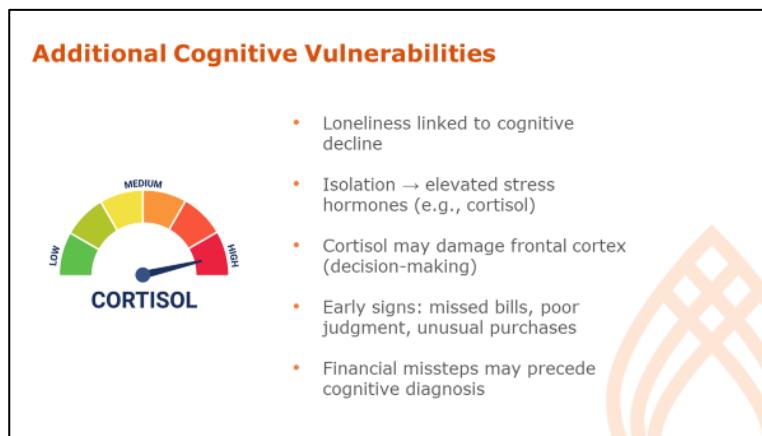
#### **Instructions:**

- **Launch** a poll (Zoom, Mentimeter, Poll Everywhere, etc.) with the following question multiple choice questions to help participants match regions of the brain to experiences associated with its cognitive decline:
  - Which brain region is most associated with emotional override and increased trust in scammers? *Answer key: Amygdala*
    - Frontal Lobe
    - Amygdala
    - Insular Cortex
    - vmPFC
  - Which brain region helps us detect risk and send a "stop" signal when something feels wrong? *Answer key: vmPFC*
    - vmPFC
    - Amygdala
    - Frontal Lobe
    - Hippocampus
  - Which brain region is tied to our "gut instinct" or intuitive danger signals? *Answer key: Insular Cortex.*
    - Insular Cortex
    - Amygdala

- Frontal Lobe
  - Cerebellum
- Which brain region is responsible for weighing long-term consequences and controlling impulses? *Answer key: Frontal Lobe*
  - Amygdala
  - vmPFC
  - Frontal Lobe
  - Brainstem
- Changes in which neurotransmitters can affect risk perception and impulse control? *Answer key: Dopamine and Serotonin*
  - Cortisol and Oxytocin
  - Dopamine and Serotonin
  - Adrenaline and GABA
  - Acetylcholine and Melatonin

*Trainer note:* After each poll, briefly review the correct answer and explain why it matters in APS casework. Reinforce that understanding these brain functions helps professionals respond with empathy and tailor interventions to cognitive needs.

## Slide #32: Additional Cognitive Vulnerabilities

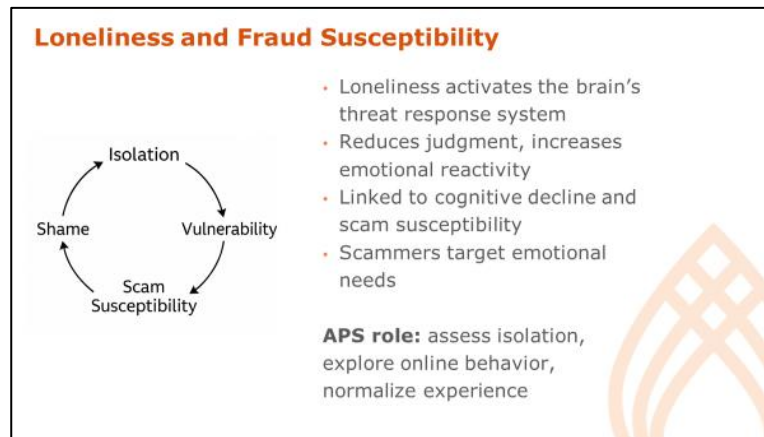


**Review** the following key concepts to clarify why each concept is important for APS professionals. These additions help reinforce the relevance of cognitive and neurological factors in scam susceptibility among older adults:

- As people age, they may experience reduced social interaction due to retirement, bereavement, mobility limitations, or geographic separation from family.
  - These changes can lead to loneliness, which is now recognized as a significant contributor to cognitive decline.
- Isolation can elevate stress hormones like cortisol, which over time may damage the frontal cortex, an area critical for decision-making and impulse control.
  - This can impair a person's ability to assess risk or recognize red flags in scam scenarios.
- Studies suggest that difficulties with financial management, such as missed bills, unusual purchases, or poor judgment, can appear years before a formal diagnosis of cognitive impairment.
  - These signs may be subtle but are important for APS professionals to recognize.

***Trainer note:** Use this slide to help participants understand that cognitive vulnerability is not always tied to a formal diagnosis. Social and emotional changes can have real neurological consequences. This understanding supports early intervention and helps frame client behavior in a nonjudgmental, trauma-informed way.*

## Slide #33: Loneliness and Fraud Susceptibility



**Share** that loneliness is not just a social issue, it has measurable effects on the brain that can increase a person's vulnerability to fraud. As APS professionals, understanding the intersection of emotional isolation and cognitive function is key to identifying risk and supporting survivors effectively.

**Review** the following key points:

- The neuroscience of loneliness and decision-making:
  - Loneliness activates the brain's threat response system, increasing emotional reactivity and reducing rational decision-making.
  - Chronic loneliness is linked to:
    - Reduced prefrontal cortex activity (affecting judgment and impulse control)
    - Increased amygdala sensitivity (heightening fear and urgency)
    - Disrupted dopamine and serotonin regulation (impacting mood and motivation)
- Cognitive decline and isolation:
  - Research shows that prolonged loneliness is associated with:
    - Decreased memory and attention
    - Reduced executive function (e.g., planning, judgment)
    - Increased risk of neurocognitive disorders (Lee et al., 2025)
  - This creates a feedback loop in which isolation can lead to cognitive decline which can lead to scam susceptibility which can lead to shame which can then lead to further isolation.
- Emotional vulnerability and scam tactics:
  - Scammers exploit emotional needs, especially the desire for connection.

- Romance scams, emergency scams, and “friendly” phishing messages often target those who are lonely or grieving.
- APS casework implications:
  - Assess for isolation in all client interviews, regardless of the allegation, as part of fraud risk screening.
  - Ask about recent losses or changes in social support.
  - Explore online behavior and consider if they are seeking connection through social media or dating apps.
  - Normalize the experience by emphasizing that loneliness is common and that scammers are skilled at exploiting it.

## Slide #34: Exploring the Digital Landscape

**Discussion: Exploring the Digital Landscape**



- What types of technology are your clients using to stay connected?
- How might these platforms increase exposure to scams like romance fraud, phishing, or emergency scams?
- What are some red flags you've seen in your casework that were linked to technology use?
- How can APS professionals support safe digital engagement while respecting autonomy?

### **Activity: Technology, Connection, and Risk – Exploring the Digital Landscape (10 minutes)**

#### ***Large Group Discussion***

**Explain** that this activity helps participants connect the concepts of social isolation, emotional vulnerability, and scam susceptibility to the real-world digital behaviors of older adults. It encourages reflection on how technology can both reduce isolation and increase exposure to fraud.

**Remind** participants that many older adults use technology to stay connected, especially when they are isolated. While this can be a protective factor, it also opens the door to new forms of manipulation.

#### **Instructions:**

- **Invite** participants to respond either in the chat or come off-mute. Use the following guiding questions:
  - *What types of technology are your clients using to stay connected (e.g., texting, social media, dating apps)?*
  - *How might these platforms increase exposure to scams like romance fraud, phishing, or emergency scams?*
  - *What are some red flags you've seen in your casework that were linked to technology use?*
  - *How can APS professionals support safe digital engagement while respecting autonomy?*

*Trainer note: Encourage participants to share real-world examples (without identifying information). If the group is quiet, offer a few examples to get the conversation started (e.g., "A client received a friend request from someone*



*claiming to be a military officer..."). Optional: Use a shared document or whiteboard (if virtual) to capture key themes.*

**Review** key takeaways:


- Technology can reduce isolation but also increase risk.
- Fraudsters often exploit emotional needs through digital platforms.
- APS professionals should assess not just whether clients are isolated, but how they are connecting and whether those connections are safe.
- Person-directed planning includes helping clients stay socially engaged while building digital literacy and fraud awareness.

## Slide #35: Barriers To Reporting

**Barriers to Reporting**

- Shame & fear may prevent disclosure
- Denial is common, especially in emotionally charged scams
- Systems are complex
- Access issues: tech, language, rural areas
- Early cognitive signs may warrant evaluation

**APS role:** support, validate, assist with reporting



**Discuss** the following key concepts:

- Age-related changes in the brain such as reduced executive function, impaired risk perception, and increased emotional reactivity, can make it difficult for older adults to recognize they've been defrauded or to act.
  - Victims may feel confused, overwhelmed, or unable to recall details clearly.
  - Shame and self-blame are common, especially when the scam involved emotional manipulation (e.g., romance or emergency scams).
  - Clients may fear being judged as incompetent or losing autonomy if they disclose what happened.
- Some clients may not accept that they were scammed, particularly if they are still emotionally invested in the relationship or opportunity. This can be compounded by cognitive decline, which may impair their ability to process contradictory information or recognize deception.
- Systemic and practical barriers:
  - Complex reporting systems (e.g., IC3, FTC) can be difficult to navigate, especially for those with limited digital literacy or cognitive impairments.
  - Law enforcement limitations: Many scams originate overseas, and local agencies may not pursue cases due to jurisdictional or resource constraints.
  - Victim-blaming language from authorities or family members can discourage disclosure.
  - Technology access: Clients in rural areas or with limited internet access may not be able to report online or seek help digitally.

- Language and communication barriers may prevent clients from understanding their options or advocating for themselves.

**Discuss** the possible APS casework implications:

- Emphasize that scams are designed to be convincing and that anyone can be targeted.
- Avoid language that implies blame or poor judgment.
- Offer to assist clients in navigating reporting portals or contacting financial institutions.
- Consider whether a referral for a cognitive evaluation is warranted if a client is unable to recognize the fraud or continues to engage with the scammer.
- Reporting creates a record and may help in future interventions even if law enforcement cannot act.

*Trainer note: This slide is a bridge between understanding the neurological and emotional impacts of fraud and planning effective, person-directed interventions. Encourage participants to reflect on how they've seen these barriers play out in their own work, and how they've helped clients overcome them.*

## Person-Directed Service Planning

**Time Allotted:** 80 Minutes


**Associated Objective(s):** Identify effective interventions to support person-directed service planning.

**Method:** Lecture, Scenario Group Work, Large Group Discussion

## Slide #36: Effective Communication with Clients

**Effective Communication with Clients**

- ✓ Create a safe, nonjudgmental space
- ✓ Use reflective listening and affirm emotions
- ✓ Normalize the experience
- ✓ Focus on scammer behavior, not client choices
- ✓ Use plain language and avoid jargon
- ✓ Allow time to process and reflect
- ✓ Highlight client strengths and resilience
- ✓ Be culturally responsive and inclusive
- ✓ Adapt to language and sensory needs



*Trainer note: this slide is animated.*

**Share** that effective communication is foundational to building trust and supporting clients in developing an individualized service plan.

**Review** key communication strategies:

- Begin by establishing a safe, non-judgmental space. Use open body language, a calm tone, and affirming language. Avoid jumping into investigative questions too quickly.
- Mirror the client's words and emotions to show understanding.
  - Ex.: *"It sounds like you were really worried when you got that call."*
- Reassure clients that fraud can happen to anyone.
  - Use phrases like: *"These scams are very sophisticated. Scammers have stolen from many people of all ages."*
- Focus on the behavior of the scammer, not the choices of the client. Avoid language that implies fault or gullibility.
  - Ex.: Instead of saying, *"Why did you send money?"* try, *"It sounds like they created a lot of pressure and urgency."*
- Avoid jargon or technical terms. Break down complex ideas into simple, digestible parts. Use analogies or examples when helpful.
  - Ex.: Instead of *"phishing,"* say, *"They sent a fake email pretending to be your bank and get your account information in order to steal your money."*
- Ask clients to explain back what they've heard in their own words. This ensures clarity and allows for correction of misunderstandings.
  - Ex.: *"Just to make sure we're on the same page—can you tell me what you understood about what we'll do next?"*
- Allow time for processing. Don't rush through explanations or decisions.

- Ex.: After discussing the scam, pause and say, *"Take your time—this is a lot to process."*
- Silence can be a powerful tool for reflection.
- Frame the client as capable and resilient. Highlight their strengths and past successes in navigating challenges.
  - Ex.: *"You did the right thing by reaching out. That takes courage, and now we can work together to protect you moving forward."*
- Be aware of cultural norms around authority, shame, money management, and family roles.
  - Ex.: In some cultures, discussing financial loss may be considered dishonorable or taboo. A client may defer all decision-making to an eldest child or spouse. In these cases, include trusted family members in the conversation (with consent) and avoid framing the scam as a personal failure.
- If the client needs access to interpretation or communication tools, ensure it's linguistically appropriate and accessible.
  - Ex.: A client may have received scam messages in their native language and may not understand the terminology used in English reporting portals like FBI's IC3 reporting system. Use plain language and offer translated materials when possible.
- Be attentive to any sensory needs the client may have.
  - Ex.: A client with hearing loss may have misunderstood a scam phone call or may struggle to follow a fast-paced discussion.
  - Use visual aids, written summaries, or slower pacing. Ask, "Would it help if I wrote this down?" or "Do you prefer to read information hear it explained, or something else?"
  - Consider asking what communication aids (i.e. eye-glasses, hearing aid, communication device etc.) the client uses and have those available for interviews and discussions.

## Slide #37: Motivational Interviewing-Inspired Approaches

Motivational Interviewing-Inspired Approaches	
When	How
Unsure if scam is real or fraudulent	Open-ended questions
Continues to engage	Affirm strengths
Resist protective actions	Reflect
Expressing mixed feelings	Summarize

***Trainer note:** This slide introduces communication strategies drawn from Motivational Interviewing (MI), a client-centered approach that supports behavior change by exploring and resolving ambivalence. While APS professionals are not expected to be clinically certified in MI, they can integrate MI-inspired techniques to build trust, reduce defensiveness, and support informed decision-making.*

**Explain** that an effective communication strategy can also be using Motivational Interviewing (MI)-inspired techniques.

**Discuss** that MI is most effective when a client is ambivalent, meaning they are uncertain, conflicted, or hesitant about changing a behavior or belief. In fraud-related APS cases, MI may be appropriate when client:

- Is unsure whether the scam was real or fraudulent.
- Continues to engage with a scammer despite warnings.
- Is unsure about protective actions (e.g., changing phone numbers, closing accounts).
- Expresses mixed feelings about involving family or accepting oversight.

**Discuss** MI-inspired techniques to build rapport and support client autonomy:

- Ask open-ended questions to encourage reflection and dialogue.
  - Ex.: "What made you feel this person was trustworthy?" or "What concerns do you have about changing your phone number?"
- Affirm client strengths to build confidence and resilience.
  - Ex.: "You've handled difficult situations before, what helped you get through those?"
- Reflect feelings and values to demonstrate empathy and understanding.

- Ex.: “It sounds like you really valued the connection you had with them, even though it turned out to be harmful.”
- Summarize key points to reinforce insights and support decision-making.
  - Ex.: “You’re saying you’re worried about losing contact with someone you cared about, but you also want to feel safe again.”

These techniques can help clients feel heard, reduce defensiveness, and increase their readiness to take protective actions.

**Share** that if a client is not ambivalent, for example if they are clear that they were scammed and want help, MI may not be necessary. Instead, focus on other techniques and task-specific interventions.

**Emphasize** that MI is not about convincing or correcting, it’s about guiding clients through their own process of change and can help clients move from uncertainty to action.



## Slide #38: Introduction to Service Planning

Introduction to Service Planning		
Person-Directed	Trauma-Informed	Culturally Responsive
Client-led goals	Emotional safety	Respect values and beliefs
Strengths-based	Avoid re-traumatization	Language access
Risk tolerance	Empowerment	Cultural Humility
Flexible planning	Normalize experience	Inclusive Communication

**Share** that after exploring how cognitive changes, emotional manipulation, and social isolation increase scam susceptibility, it's essential to shift toward restoring safety, dignity, and control.

Service planning in APS is a collaborative, individualized process that identifies a survivor's needs, strengths, and goals, and develops a tailored plan of support that promotes safety, well-being, and self-determination.

**Discuss** the core principles of a service plan:

- Person-Directed:
  - Focus on the individual's goals, values, strengths, and preferences, as they define them.
  - Involve the client in all decisions and respect their right to take risks.
  - Build on existing strengths and support systems.
  - Avoid "one-size-fits-all" solutions, plans should reflect the person's unique context and allow for flexibility to adjust as interventions are implemented (or not).
    - This includes any cognitive deficits that may complicate decision-making or require family/caregivers' approvals to intervene.
  - *Trainer note: why we are using "person-directed" versus "person-centered"*
    - *The client is an active participant in planning for their case, so they are driving their service plan. Whereas "centered" may imply they are a more passive participant. We want to facilitate buy-in versus reluctance.*
    - *Being person-directed is an empowering process.*
- Trauma-Informed:

- Recognize that fraud can be a traumatic experience, often involving betrayal, shame, and loss. This can include significantly diminished economic circumstances that may necessitate lifestyle changes.
- Prioritize emotional safety and avoid re-traumatization:
  - Do not blame the victim
  - Put the responsibility for the scam or fraud on the perpetrator
  - Minimize the number of times the victim is interviewed
    - APS interview can be conducted concurrently with law enforcement
- Use empowering language and validate the survivor's experience.
- Offer choices and control wherever possible to restore a sense of agency.
- Be alert to any mental health conditions which can result from the scam (ex. suicidal ideation, depression, anxiety, etc.) and make appropriate referrals or interventions.
- Recognize trauma responses
- Culturally Responsive:
  - Explore what is important to the person, including how their values and culture may impact planned interventions.
  - Acknowledge and respect cultural values, beliefs, and communication styles.
  - Understand that cultural norms may influence help-seeking behaviors, trust in institutions, or family roles. Inquire directly about the person's views of cultural norms.
  - Use interpreters or cultural brokers when needed.
  - Avoid assumptions—ask open-ended questions to understand the survivor's worldview.

**Encourage** participants to reflect on how they can adapt their planning approach to meet each client where they are, especially when shame, confusion, or cultural differences are present. This slide prepares participants to apply these principles in the upcoming case scenario activity.

## Slide #39: Fraud Recovery Service Planning



Use the **Handout: Fraud Recovery Service Planning** to **review** the following key elements of a scam-informed and person-directed service plan:

- Safety planning:
  - First address immediate risk and needs (e.g., stopping or reversing a pending transaction, ensuring basic needs are met)
  - Address ongoing risks (e.g., continued contact with scammer, financial access).
  - Include digital safety strategies (e.g., password changes, scam blocking tools, phone number change).
- Emotional support:
  - Normalize feelings of shame, grief, or betrayal.
  - Refer to counseling or peer support groups if appropriate.
- Financial recovery and oversight:
  - Connect with financial institutions, credit monitoring, or fiduciary services.
  - Explore voluntary financial oversight options (e.g., trusted family member, POA).
  - Use involuntary interventions only when all other alternatives have been explored and/or the person lacks decision-making ability and is at continued risk of harm.
    - In California an involuntary intervention may be warranted when a person is unable to resist undue influence, even if they retain decision-making ability. (*If training outside of California, check local statutes and policies*)
- Social connection:
  - Reduce isolation by connecting to community programs, community centers, or virtual groups.

- Education and empowerment:
  - Provide scam prevention resources and digital literacy support.
  - Encourage safe online behaviors and critical thinking.
- Cognitive and ability considerations:
  - Screen for decision-making ability.
  - Involve healthcare providers or neuropsychological evaluation as needed.

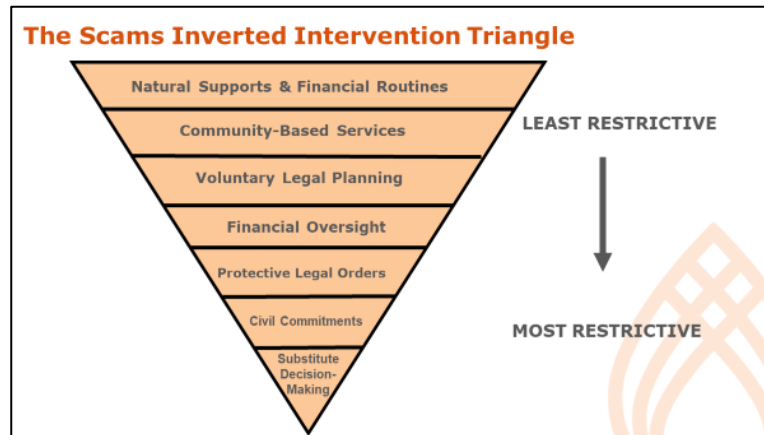
**Emphasize** that effective service planning is not just about stopping the scam, it's about helping the client recover, rebuild, and remain empowered.

**Encourage** participants to reflect on how the aging brain, emotional trauma, and cultural context all shape the planning process.

## Handout: Fraud Recovery Service Planning

Service Plan Element	Strategies
<i>Safety Planning</i>	<p>First address immediate risk and needs (e.g., stopping or reversing a pending transaction, ensuring basic needs are met)</p> <p>Address ongoing risks (e.g., continued contact with scammer, financial access).</p> <p>Include digital safety strategies (e.g., password changes, scam blocking tools, phone number change).</p>
<i>Emotional Support</i>	<p>Normalize feelings of shame, grief, or betrayal.</p> <p>Refer to counseling or peer support groups if appropriate.</p>
<i>Financial Recovery and Oversight</i>	<p>Connect with financial institutions, credit monitoring, or fiduciary services.</p> <p>Explore voluntary financial oversight options (e.g., trusted family member, POA).</p> <p>Use involuntary interventions only when all other alternatives have been explored and/or the person lacks decision-making ability and is at continued risk of harm.</p>
<i>Social Connection</i>	<p>Reduce isolation by connecting to community programs, community centers, or virtual groups.</p>
<i>Education and Empowerment</i>	<p>Provide scam prevention resources and digital literacy support.</p> <p>Encourage safe online behaviors and critical thinking.</p>
<i>Cognitive and Ability Considerations</i>	<p>Screen for decision-making ability.</p> <p>Involve healthcare providers or neuropsychological evaluation as needed.</p>

## Slide #40: The Scams Inverted Intervention Triangle



*Trainer note:* Use the visual triangle to walk participants through each level of intervention. Encourage discussion about how these levels show up in real-world casework. Reinforce that least restrictive does not mean ineffective, in many cases, informal supports and community services are the most appropriate and sustainable solutions. Following this overview, the training will explore how to apply this framework when working with clients who retain or lack decision-making capacity, including how to assess capacity and select appropriate interventions.

**Share** that whether or not a person has the cognitive ability to make their own decisions, in APS work, we must always consider voluntary and least restrictive interventions prior to seeking most restrictive or involuntary interventions. APS professionals are often tasked with balancing two core responsibilities:

- Protecting older adults and adults with disabilities from harm
- Upholding their right to autonomy and self-determination

**Introduce** the Scams Inverted Intervention Triangle which can be used as a visual and conceptual guide to navigating this balance. This model illustrates a continuum of interventions, organized from least to most restrictive. While it emphasizes autonomy and safety, it also supports a harm reduction approach, especially when clients are not ready or willing to disengage from a scam.

**Explain** the structure and purpose of the triangle:

- The triangle is inverted to emphasize that most clients can be supported effectively using the broader, less intrusive strategies at the top.

- As risk increases or decision-making ability decreases, more directive interventions may be required.
- These more restrictive options should be considered only as a last resort.

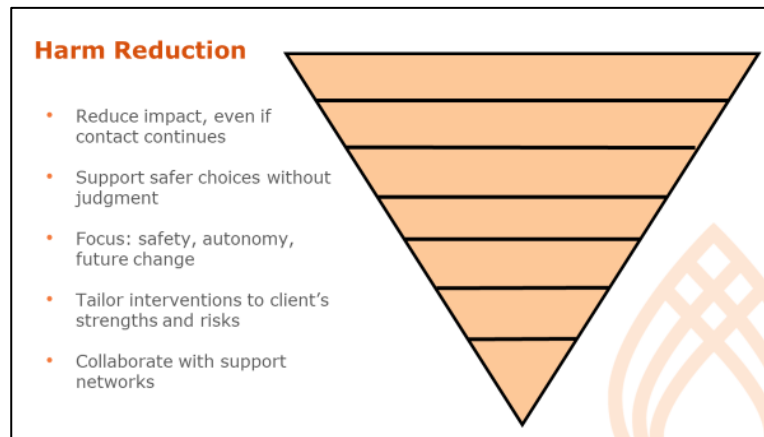
**Clarify** why least restrictive options are preferred:

- Less restrictive options can utilize existing supports and trusted relationships to reduce harm, both financial and emotional. They allow for the person's autonomy self-determination.
- More restrictive interventions often involve:
  - Legal oversight
  - Loss of personal autonomy
  - Disruption to the client's sense of control, identity, and dignity
- APS professionals should seek to preserve independence and decision-making authority whenever possible.
- Interventions should be tailored to the client's needs, strengths, and preferences.

**Review** key principles of interventions:

- Start with the least restrictive option that effectively addresses the client's needs and risks.
- Progress only as necessary, based on the client's ability, preferences, and the severity of harm or risk.
- Involve the client in decision-making to the greatest extent possible, even when protective interventions are required.
- Document the rationale for any movement toward more restrictive interventions, including efforts made to use less intrusive options.

## Slide #41: Harm Reduction



*Trainer note: this slide is animated.*

**Explain** that harm reduction in APS fraud cases means working with the client to reduce the impact of the scam, even if they are still engaging with the perpetrator. This may include:

- Setting spending limits or alerts on accounts
- Encouraging safer communication practices
- Providing education on scam tactics without judgment
- Supporting emotional and social needs to reduce isolation

**Share** that harm reduction is:

- Especially useful when clients are not ambivalent.
- A way to support safety by reducing harm and planting seeds for future change.

**Discuss** application in APS casework:

- Identify appropriate interventions based on the client's current strengths, risks, and decision-making ability.
- Collaborate with clients and their support networks to build plans that promote safety without unnecessary loss of autonomy.
- Recognize when legal or protective actions are warranted and how to implement them in a trauma-informed, culturally responsive manner.

**Activity: Interventions Brainstorm – Least to Most Restrictive (10-15 minutes)**

***Virtual Whiteboard and Large Group Discussion***



**Introduce** that the purpose of this activity is to help participants internalize the concept of least-to-most restrictive interventions by brainstorming real-world examples from their own practice and mapping them to the appropriate level of the triangle.

**Instructions:**

- **Display** a blank triangle on a shared whiteboard or screen (Interactive Whiteboard such as Miro, Zoom Whiteboard, Mural) or Shared Document. Also **display** the labeled version of the triangle with only the level titles:
  - Natural Supports & Financial Routines
  - Community-Based Services
  - Voluntary Legal Planning
  - Financial Oversight
  - Protective Legal Orders
  - Civil Commitments
  - Substitute Decision-Making
- **Prompt** participants to brainstorm examples of interventions they've used or seen in APS casework and place them in the appropriate level of the triangle. **Encourage** participants to think broadly, including informal supports, digital tools, legal mechanisms, and culturally specific practices.
- After 5–7 minutes of brainstorming, **review** the completed triangle together.

Below is a sample answer key to help guide debrief:

Level	Example Interventions
Natural Supports & Financial Routines	Trusted family check-ins, automatic bill pay, daily money management apps, informal caregiver reminders
Community-Based Services	Community centers, Meals on Wheels, housing navigation, lifeline alert systems
Voluntary Legal Planning	Power of Attorney, Advance Health Care Directive, Living Trust
Financial Oversight	Representative Payee (SSI), VA Fiduciary, joint bank account with monitoring
Protective Legal Orders	Restraining order against scammer, order for protection from financial abuse
Civil Commitments	Mental health or substance use commitment under state law
Substitute Decision-Making	Conservatorship, Guardianship (financial or full)

**Debrief** questions for large group discussion:

- How do we decide when to move from one level to the next?
- How might cultural values or client preferences influence where we start on the triangle?

## Slide #42: Cognitive and Behavioral Strategies



**Share** that these strategies are especially helpful for clients who may not meet the threshold for cognitive impairment but are showing early signs of decision-making difficulty, emotional vulnerability, or overreliance on digital interactions.

**Review** the following cognitive (mental) and behavioral (action) support strategies in service planning:

- Encourage in-person social engagement:
  - Help clients reconnect with trusted individuals and community spaces to reduce isolation and increase protective social contact.
  - *Ex.: community centers, community events, family visits, or faith-based gatherings.*
- Rebuild joy and identity through hobbies:
  - Support clients in rediscovering activities that bring meaning and structure.
  - *Ex.: Listening to music, gardening, reading, crafting, or volunteering.*
- Promote routine-building and goal-setting:
  - Establishing daily routines and small, achievable goals can reduce unstructured time spent online and improve cognitive resilience.
  - *Ex.: Setting a weekly schedule, creating a morning routine, or planning regular outings.*
- Support financial structure and oversight:
  - Help clients develop or re-establish financial routines that reduce impulsive or risky behavior.
  - *Ex.:*
    - *Creating a monthly budget*
    - *Meeting with a financial counselor*
    - *Setting up automatic bill pay*


- *Exploring voluntary oversight options (e.g., trusted family member or POA)*
- Provide digital literacy and scam prevention education:
  - Build confidence and reduce risk by helping clients understand how to safely navigate online spaces.
  - *Ex.:*
    - *Teaching how to recognize scam messages*
    - *Reviewing privacy settings on social media*
    - *Practicing how to verify suspicious emails or texts*

## Slide #43: Interventions for Clients with Decision-Making Ability

**Interventions for Clients with Decision-Making Ability**

- Auto bill pay to reduce missed payments and impulsive spending
- Monitoring accounts with a trusted support person
- Representative Payee for Social Security or SSI benefits
- Financial guardian for veterans benefits
- Spending alerts or transaction limits through financial institutions
- Referral to financial counseling or fiduciary services
- Education on scam prevention and digital safety tools
- Coordination with community-based programs to reduce isolation and increase protective social contact

**Additional Strategies to Consider**



**Share** that APS professionals should begin with the least restrictive interventions that effectively address the client's immediate and ongoing needs, even when more protective or involuntary actions may eventually be necessary. This approach ensures that autonomy is respected and that interventions are scaled appropriately to the level of risk.

**Ask** participants to consider the immediate impact. In cases of active financial exploitation, APS professionals should begin with urgent protective steps. These may include working with financial institutions to reverse transactions, closing compromised accounts, canceling credit cards, and ensuring the perpetrator no longer has access to the client's finances. These actions are critical to stopping further harm and stabilizing the situation. While these steps are not inherently restrictive, they must be taken with the client's consent and involvement whenever possible.

**Discuss** how once immediate harm is addressed, APS professionals can use the triangle to guide longer-term planning:

- Starting at the top, interventions may include encouraging financial planning (e.g., drafting a will, identifying a future decision-maker, creating a healthcare directive).
- If the client has a diagnosis of a cognitive impairment or a diagnosis of a neurocognitive disorder, they may choose to involve a trusted family member to monitor accounts or flag suspicious activity. These voluntary steps preserve autonomy while reducing risk.
- If the client refuses to acknowledge the scam and has experienced substantial financial loss, a neurocognitive evaluation may be warranted to assess for underlying impairment. Barriers to this may include cost or

waitlists, and APS may need to advocate for access to medical and insurance resources.

**Discuss** additional interventions to consider:

- Auto bill pay to reduce missed payments and impulsive spending
- Monitoring accounts with a trusted support person
- Representative Payee for Social Security or SSI benefits
- Financial guardian for veterans benefits
- Substitute decision-makers (e.g., POA) should keep the client involved in planning and decisions whenever possible
- Use of spending alerts or transaction limits through financial institutions
- Referral to financial counseling or fiduciary services
- Education on scam prevention and digital safety tools
- Coordination with community-based programs to reduce isolation and increase protective social contact

## Slide #44: Interventions for Clients Without Decision-Making Ability

**Clients without Decision-Making Ability**

**Strategies**

- Use least restrictive options first
- Presume ability unless formally assessed
- Include clients in decisions when possible
- Document thoroughly
- Assess decision-making ability
- Consider POA, Representative Payee, or Conservatorship
- Apply financial safeguards
- Ensure digital safety
- Provide emotional support and connect to mental health services



**Share** that when a client lacks the ability to make informed decisions due to cognitive impairment, neurocognitive disorders, or other factors, APS professionals may need to introduce more involuntary protective interventions. These actions should still be grounded in a supportive, person-directed approach that honors the client's dignity, preferences, and emotional needs. The goal is to balance the client's right to autonomy with their safety and well-being, using the least restrictive and most empowering strategies available.

**Revisit** the inverted triangle and discuss the guiding principles for intervention:

- Always begin with the least intrusive option that ensures safety.
- Presume decisional capacity unless proven otherwise: Use screening tools and referrals for formal assessments when needed.
- Even when decision-making ability is limited, include the client in discussions and decisions to the extent they are able.
- Clearly record observations, assessments, and rationale for any protective interventions.

**Discuss** the following intervention strategies for clients when decision-making ability is of concern:

- Capacity Assessment for Financial Decision-Making:
  - Collaborate with healthcare providers to determine if the client can understand, balance risk and benefits, and reason through decisions.
  - Refer for a formal neuropsychological or medical evaluation.
- Substitute Decision-Making:
  - Power of Attorney (POA): If the client still has decisional capacity, encourage them to designate a trusted person.

- Representative Payee: For clients receiving Social Security or VA benefits, consider appointing a payee to manage funds.
  - Conservatorship/Guardianship: If decisional capacity is lost and no POA exists, initiate conservatorship proceedings as a last resort.
- Financial Safeguards:
  - Work with financial institutions to freeze or monitor accounts.
  - Set up automatic bill pay or limited-access debit cards.
  - Identify a trusted substitute decision maker.
  - Involve fiduciary services or public guardians when appropriate.
- Environmental and Digital Safety:
  - Remove access to devices or accounts used in scams with client permission or legal authority.
  - Install scam-blocking tools or filters.
  - Limit unsupervised internet use if it poses a risk.
- Emotional and Social Support:
  - Engage family or caregivers in emotional support and education.
  - Connect to adult day programs or supervised social activities to reduce isolation.
  - Refer to mental health programs if the person is exhibiting signs of anxiety, depression, social isolation, suicidal ideation, etc.




## Slide #45: Activity – Without Decision Making Ability

**Activity: Without Decision-Making Ability**

*Maria is an 84-year-old woman with moderate neurocognitive disorder who has sent over \$10,000 to a romance scammer. She believes she is engaged to the man and refuses to stop contact. Her son has Power of Attorney but is unsure how to intervene.*

**Discuss** | What are the next steps?  
How would you coach the son?



### **Activity: Without Decision Making Ability (5 minutes)**

#### ***Large Group Discussion***

**Use** a brief case scenario to illustrate how these interventions might unfold. For example: “Maria is an 84-year-old woman with moderate neurocognitive disorder who has sent over \$10,000 to a romance scammer. She believes she is engaged to the man and refuses to stop contact. Her son has Power of Attorney but is unsure how to intervene.”

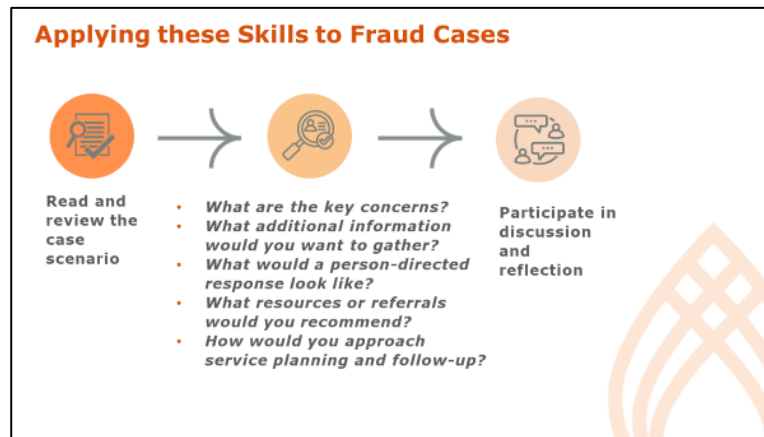
**Ask** participants:

- What are the next steps, and how would you coach the son?

Below are example **discussion** points:

- Encourage the son to contact his attorney to understand what he is legally able to do in terms of him managing his mother’s money.
- Refer Maria for a follow-up a neurocognitive evaluation.
- Determine whether the son is able to freeze or close Maria’s account that the money is being taken from.
- Make a police report if one has not already been made.
- Encourage the son to take over the bill paying but involve his mother as much as possible, such as bill paying and discussing finances together.
- Consider changing Maria’s phone number.
- The son could try and engage other family members in calling and visiting his mother to reduce isolation.
- Consideration of referring his mother to an older adult day program or hiring a care giver
- Taking away electronic devices would be the very last step.

## Slide #46: Applying These Skills to Fraud Cases



### **Activity: Applying Skills to Fraud Cases (20-30 minutes)**

#### ***Small Breakout Group Discussions***

**Let** participants know they will now apply what they've learned to case scenarios involving older adults who may have experienced fraud.

#### **Instructions:**

- **Assign** participants to breakout rooms (3–5 people per group). Each group will receive one case from the **Handout: Case Scenarios**.
- **Tell** groups they will have 10 minutes to read the assigned case together and then **discuss** the following:
  - *What are the key concerns in this case?*
  - *What additional information would you want to gather?*
  - *What would a person-directed response look like?*
  - *What resources or referrals would you recommend?*
  - *How would you approach service planning and follow-up?*
- Spend 10 minutes **debriefing** as a large group. **Summarize** each scenario and **ask** each group to share one insight, challenge, or creative solution from their discussion, using the Trainer note to guide and deepen the conversation.

*Trainer note: the following notes are potential points of discussion following small group breakouts. Use these notes to help facilitate a report out and ensure all key points are covered.*

#### Points of discussion for Case Scenario 1 with Bill:

- *Building Rapport & Gentle Inquiry:*
  - *Explain your role as an APS professional.*

- *Open ended questions to learn more about him and his situation. Connect on what is of interest to that person.*
- *Acknowledge his desire for companionship and connection. Avoid direct accusations or judgment*
- *Inquire about supports. For example, who would he turn to for help if he needed to, and if he has family support.*
- *Inquire about the specifics of the relationship, and if she has made any other financial requests, the amounts of money involved, and the methods of transfer.*
- *Explain common tactics of online romance scams, where fraudsters cultivate emotional relationships to extract money. Share examples of similar cases (without identifying information) to normalize the experience and reduce shame.*
- *Financial Assessment & Intervention:*
  - *With his permission, review his bank statements or financial records (or encourage his supports to do so with his consent).*
  - *Document the pattern of withdrawals/transfers.*
  - *Point out that this has every indication of being a romance scam.*
  - *Advise him to cease all communication and money transfers to the woman. This may include changing phone numbers, disabling social media accounts, removing apps like WhatsApp.*
  - *If money has been sent via wire transfer, instruct him to contact his bank immediately to see if any funds can be recalled (unlikely but worth trying).*
  - *Help him report the scam to the FBI's Internet Crime Complaint Center (IC3).*
  - *Find out if he has given any of his account information or password to the woman. If so, recommend that he work with his bank to close the account and open a new account. Remind him not to give his account information to anyone in the future.*
- *Engagement & Support:*
  - *Facilitate a conversation between him and his trusted supports (with his consent) to discuss their concerns and potential financial risks.*
  - *Explore options for financial oversight, such as adding a trusted family member to his bank accounts for monitoring (with appropriate safeguards) or establishing a power of attorney for financial matters if he is agreeable and understands the implications.*
- *Addressing Underlying Needs:*
  - *Recognize his loneliness as a vulnerability. Connect him with local social groups or other community activities that can foster genuine connections and reduce isolation.*
  - *Consider a neurocognitive assessment if there are concerns about his decision-making ability or increased susceptibility to manipulation.*

Points of discussion for Case Scenario 2 with Eden:

- *Immediate Action:*
  - *Reassure her and validate her concerns.*
  - *Explain the common "grandparent scam" and how it preys on emotional connections and urgency.*
  - *Recommend her not to purchase any more gift cards and not to send the ones she already bought.*
  - *Help her attempt to contact her actual granddaughter (or her granddaughter's parents if she is unavailable) to verify her whereabouts and safety.*
- *Investigation and Interventions:*
  - *If the scam is confirmed, guide her on how to report the incident to local law enforcement (non-emergency line) and the Federal Trade Commission (FTC). Provide any assistance needed to make the reports.*
  - *Assess how far the damage has gone. For example, has she given anyone else her bank account information, any passwords, etc. If so, she will need to contact financial institutions and change account passwords.*
  - *Educate her on common red flags of scams (urgency, secrecy, demanding specific payment methods like gift cards/wire transfers, threats).*
  - *Discuss strategies for verifying callers' identities, such as establishing a "code word" with family members for urgent situations.*
  - *Suggest blocking unknown numbers or using call screening services if available.*
  - *May need to consult with clients' family and physician to determine if she has financial decision-making ability.*
- *Ongoing Support:*
  - *Monitor her for signs of continued distress or targeting.*
  - *Explore opportunities to reduce her social isolation, which can make individuals more vulnerable (e.g., connecting her with community centers, volunteer opportunities, or regular check-ins from community groups and family members).*
  - *Discuss potential power of attorney or financial management arrangements with her and her family if this becomes a recurring issue or her cognitive abilities decline.*
  - *If Eden does not have decision-making ability, financial management arrangements specifically with state statute may need to be enacted.*

Points of discussion for Case Scenario 3 with Mateo:

- *Immediate Measures:*
  - *Build rapport by acknowledging his frustration and the violation of his trust. Reassure him that these scams are sophisticated and target many people.*
  - *Recommend him to immediately disconnect his computer from the internet (unplug ethernet, turn off Wi-Fi) to help ensure cybersecurity.*
  - *Advise them both to change all online passwords, starting with their banking, email, and any other sensitive accounts, using a separate, secure device (e.g., a friend's computer, a public library computer, or his phone not connected to his home Wi-Fi).*
  - *Contact the bank and credit card companies to report potential unauthorized access and monitor his accounts for suspicious activity.*
  - *Consider placing a fraud alert on their credit.*
- *Reporting and Recovery:*
  - *Help them report the incident to the FTC and IC3.*
  - *Explain that legitimate tech companies do not initiate contact with pop-ups demanding payment or remote access.*
  - *Advise him to take his computer to a reputable local computer repair shop to have it thoroughly scanned for malware and to remove any remote access software installed by the scammers.*
- *Prevention and Education:*
  - *Educate him and his spouse on common tech support scam tactics: unsolicited pop-ups, urgent warnings, demands for immediate payment or remote access, and use of gift cards for payment.*
  - *Emphasize that he should never grant remote access to his computer to an unsolicited caller or pop-up.*
  - *Recommend using reputable antivirus software and keeping it updated.*
  - *Suggest bookmarking official tech support numbers for his devices/software so he can verify them independently.*
  - *If the client and his wife have low technology literacy or ability, discuss if they have a trusted support (e.g. adult child or grandchild who can help them to perform needed tasks).*

## Handout: Case Scenarios

### Case Example 1:

*Bill Z. is a 72-year-old man who was referred to APS following concerns about possible financial exploitation. He has been widowed for eight months and is recovering from a hip fracture that has left him with limited mobility. Due to ongoing post-surgical complications, he receives part-time support from a caregiver. His adult daughter lives nearby, but they have limited contact.*

*Recently, Bill shared with his caregiver that he has developed a close online relationship with a woman he met through Facebook. He describes her as being in her 40s, living in Ukraine, and hoping to come to the U.S. for safety. They communicate frequently via Facebook Messenger, and she encouraged him to download WhatsApp to stay in closer contact.*

*Bill's caregiver became concerned after he shared that he had transferred \$5,000 in cryptocurrency to an unfamiliar account. When asked, Bill explained that the money was to help his girlfriend purchase a plane ticket to the U.S. and that he planned to send more funds to "keep her safe." The caregiver, recognizing the signs of a potential romance scam, filed a report with APS.*

### Discussion Questions:

- *What are the key concerns in this case?*
- *What additional information would you want to gather?*
- *What would a person-directed response look like?*
- *What resources or referrals would you recommend?*
- *How would you approach service planning and follow-up?*

**Case Example 2:**

Eden L. is an 80-year-old woman who was referred to APS following concerns about possible financial exploitation. She has recently exhibited early signs of a neurocognitive disorder and reports feeling “not quite herself” since a recent change in her blood pressure medication. Eden also experiences age-related hearing loss, which makes phone communication challenging.

During a home visit, Eden asks for help purchasing additional gift cards. She explains that her granddaughter has been arrested in Mexico City and needs money for bail. Eden says she received a phone call from someone claiming to be the police, and then spoke directly with her granddaughter, who begged her not to tell her parents. Eden has already mailed one set of gift cards and has purchased more.

A local drugstore manager, concerned by the unusual volume and urgency of Eden’s purchases, contacted APS. When the manager gently explained that this situation matched a known scam pattern, Eden insisted it was real, saying, “My granddaughter needs me. I have to help her.”

**Discussion Questions:**

- *What is the role of the APS professional?*
- *What information do you still need?*
- *What are your first steps?*
- *How will you address the financial harm given the diagnosed neurocognitive disorder?*
- *How will you reduce the risk of recurrence?*
- *What if the client is initially resistant to this being a scam?*



**Case Example 3:**

Mateo A. is a 68-year-old man who was referred to APS for concerns of possible financial exploitation and the need for protective interventions. He lives in a multigenerational household with his 66-year-old wife, Elena, who works part-time at a local community center. Mateo is retired and spends much of his time at home managing household tasks and staying connected online. He has chronic obstructive pulmonary disease (COPD), which has impacted his memory and cognitive processing, particularly when he is fatigued or experiencing shortness of breath.

Mateo is bilingual but more comfortable speaking Spanish. He can read and write in English but struggles with complex written materials, especially those involving financial or technical language. During your visit, Mateo appears friendly and cooperative but somewhat confused when discussing a recent phone call he received from someone claiming to be from a software's technical support. The caller told him that his computer was infected with a virus and offered to fix the issue remotely for a fee. Trusting the caller, Mateo paid \$200 using his debit card and allowed the individual to access his computer to install what he believed was antivirus software.

Mateo explains that his computer had been running slowly, so the call seemed legitimate. However, he now feels unsure about what was installed and why the caller contacted him in the first place. Elena, his wife, later noticed a suspicious withdrawal from their joint checking account and contacted the bank. When the bank representative advised her to close the account and open a new one, she hesitated, expressing uncertainty about making financial decisions without Mateo's input. She was also unsure how to explain the situation to him in a way that wouldn't cause distress.

The bank filed a report with APS, expressing concern that the couple may be at continued risk of financial exploitation. The representative noted that additional unauthorized withdrawals could occur if the fraudster retained access to their account or computer.

*Discussion Questions:*

- *What is the role of the APS professional?*
- *What information is still needed?*
- *What are your first steps?*
- *How will you address the financial harm?*
- *What if the client is initially resistant to this being a scam?*



## Wrap-Up

**Time Allotted:** 15 Minutes

**Associated Objective(s):** N/A


**Method:** Summary and Closing

---

## Slide #47: Review and Summary

**Review and Summary**

- Fraud schemes exploit trust, urgency, and emotion
- Brain changes increase scam susceptibility
- Emotional harm leads to shame, fear, and isolation
- Barriers to reporting include denial, tech access, and stigma
- Trauma-informed communication builds trust
- Service plans must reflect values, culture, and ability



*Trainer note: This slide is designed to consolidate learning, reinforce key takeaways, and provide closure to the training. Invite participants to reflect on how they will apply what they've learned in their APS practice.*

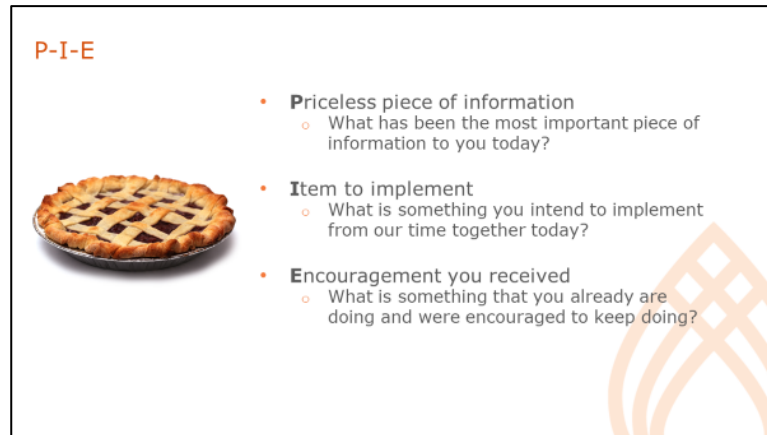
### **Key** themes to review:

- Explored the wide range of fraud schemes targeting older and dependent adults, and how scammers use social engineering, urgency, and emotional manipulation to exploit trust and vulnerability.
- Examined how age-related changes in brain function, particularly in the prefrontal cortex, amygdala, and insular cortex, can impair risk detection, emotional regulation, and decision-making. These neurological shifts, combined with social isolation and emotional needs, increase susceptibility to fraud.
- Fraud victimization is not only financial, it often results in shame, grief, fear, and social withdrawal.
- Discussed the cognitive, emotional, and systemic barriers that prevent clients from recognizing or reporting fraud. These include denial, shame, fear of losing autonomy, and difficulty navigating complex reporting systems.
- Reviewed trauma-informed, culturally responsive communication techniques tailored to fraud survivors. These included tools to help reduce defensiveness like reflective listening, normalization, plain language, and empowering dialogue.
- Identified how to develop individualized, scam-informed service plans that address safety, emotional recovery, financial oversight, and social connection.

- Explored how MI techniques can support clients who are ambivalent about change, especially those still engaged with scammers or unsure about taking protective steps.
- Identified practical strategies to reduce risk and promote resilience, including routine-building, digital literacy education, financial planning, and reconnection with meaningful activities and relationships.

**Invite** participants to ask questions about any part of the training. **Use** this time to clarify concepts, revisit complex topics, or explore how the material applies to specific case scenarios.

## Slide #48: P.I.E.



**Inform** participants that we'll wrap up the day by reflecting on their experience.

**Ask** participants to silently take five (5) minutes to answer the following questions, on their own. Those who want to share can do so after everyone's had the time to individually answer.

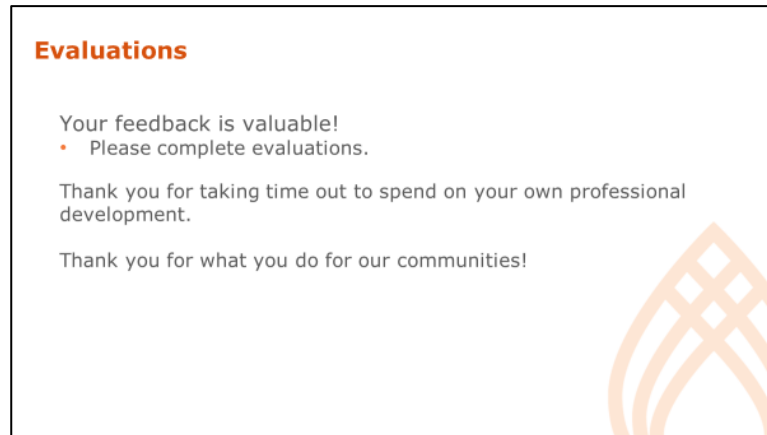
1. P- Priceless piece of information. What has been the most important piece of information to you today?
2. I- Item to implement. What is something you intend to implement from our time today?
3. E- Encouragement I received. What is something that I am already doing that I was encouraged to keep on doing?

Once complete, **ask** for volunteers to share what they wrote down for each reflection.

If time allows, **debrief** with the following questions:

- What are some of the key words that you heard while you shared?
- What were the common themes that kept coming up?
- What would it mean for APS if we implemented the things on your PIE?
- What would it mean for APS if we did not implement the things on your PIE?

## Slide #49: Evaluations



**Provide** information on how to complete evaluations.

**Thank** participants for taking time out of their day for their own professional development and dedication to support older adults and adults with disabilities.

## Appendix: Resource Handout

**AARP Scams & Fraud Network:** <https://www.aarp.org/money/scams-fraud/>

The AARP operates an information portal for different forms of fraud and scams, including a fraud watch network that enables reporting for different forms of fraud and tailored resources for victims. This includes briefs on different forms of fraud and scams and ways to detect them among older populations.

**California Department of Financial Protection and Innovation:**  
<https://dfpi.ca.gov/news/insights/preventing-and-reporting-elder-financial-abuse/>

The California Department of Financial Protection offers a resource portal for seniors who experience different forms of scams and abuse.

**California State Attorney General Office, Cybercrime Section:**  
<https://oag.ca.gov/cybercrime>

The Cybercrime Section of the State AG's office deals with different forms of cybercrime and fraud, and can aid victims of identity theft through their online portal. They offer a detailed breakdown of strategies to protect your identity, and operate the California Identity Theft Registry for victims of identity theft to aid in reducing their risk of future victimization.

**Coinbase Asset Recovery:** <https://help.coinbase.com/en/coinbase/trading-and-funding/sending-or-receiving-cryptocurrency/recover-unsupported-crypto>

The cryptocurrency platform Coinbase can provide asset recovery services in limited circumstances to aid clients who have lost cryptocurrency.

**FBI Elder Fraud Section:** <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/elder-fraud>

This website provides various resources for the public to understand different scams and frauds targeting seniors.

**FTC Identity Theft Reporting Portal:** <https://www.identitytheft.gov/>

This platform is operated by the Federal Trade Commission and provides a reporting platform for identity theft. Victims can file a report here and get personalized information that can be used to recover from the event, including pre-populated form letters for creditors, banks, etc.

**FTC Identity Theft Resource Center:** <https://www.idtheftcenter.org/>

This platform is operated by the Federal Trade Commission and provides resources and information for victims of different forms of identity theft and fraud. They provide detailed, simple to understand reports on how to deal with different kinds of crime involving personal identity details, such as credit histories and bank accounts.

**Internal Revenue Service (IRS) Identity Theft Central:**

<https://www.irs.gov/identity-theft-central>

Provides resources and reporting for victims of tax fraud, when someone has used your identity information to commit tax fraud.

**Internet Crime Complaint Center (IC3):** <https://www.ic3.gov>

The IC3 is the premier online reporting platform for victims of economic cybercrimes, particularly frauds. Victims can file complaints through their online portal, which is managed by the Federal Bureau of Investigation, which may be triaged and sent to relevant law enforcement agencies for follow up. They also provide regular briefs and short-form articles on current threats and scams targeting different groups.

**National Elder Fraud Hotline:** <https://ovc.ojp.gov/program/stop-elder-fraud/providing-help-restoring-hope>

The Office for Victims of Crime provides a fraud hotline that can be used to support older people who have been victimized in different ways. The hotline and other resources can be found at this website.

**The US Department of Justice Elder Justice Initiative:**

<https://www.justice.gov/elderjustice/senior-scam-alert>

The federal US Department of Justice operates a resource and information portal for seniors who may experience different forms of fraud, scams, and abuse.

## References

Anderson, M. & Perrin, A. (2017). Tech adoption climbs among older adults. May 17, 2017. Pew Research Center.

<https://www.pewresearch.org/internet/2017/05/17/technology-use-among-seniors/>

Andonellis, M. (2022). Putting your heart and wallet on the line: How to combat romance scams targeting the elderly. *Elder LJ*, 30, 135.

BBB Institute for Marketplace Trust. (2024). 2024 BBB Scam Tracker risk report. <https://bbbmarketplacetrust.org/wp-content/uploads/2025/02/2024-RiskReport-US.pdf>

Better Business Bureau Marketplace Trust. (n.d.). *Scam type glossary*. Scam Survival Toolkit. <https://scamsurvivaltoolkit.bbbmarketplacetrust.org/scam-type-glossary/>

Boyle, P. A., Yu, L., Schneider, J. A., Wilson, R. S., & Bennett, D. A. (2019). Scam awareness related to incident Alzheimer dementia and mild cognitive impairment: A prospective cohort study. *Annals of Internal Medicine*, 170(10), 702–709.

Carlson, C., & Kerzner, L. (2024, November 19). *Why so many seniors get swindled: The biology of financial vulnerability* [PowerPoint slides]. Hennepin County Adult Protection Program & Hennepin Healthcare.

Cross, C. (2016). 'They're very lonely': Understanding the fraud victimization of seniors. *International Journal for Crime, Justice and Social Democracy*, 5(4), 60–75.

Cross, C. (2017). 'But I've never sent them any personal details apart from my driver's license number...': Exploring seniors' attitudes towards identity crime. *Security Journal*, 30, 74–88.

Cross, C. & Holt, T. J. (2025). Does age matter? Examining seniors' experiences of romance fraud. *Security Journal*, 38, 46.

Dahl, M.J., Bachman, S.L., Dutt, S. *et al.* (2023). The integrity of dopaminergic and noradrenergic brain regions is associated with different aspects of late-life memory performance. *Nature Aging* 3, 1128–1143.

DeLiema, M., Fletcher, E., Honick, C., Martindale, J., McDowell, J., Mottola, G., & Pessanha, R. (2025). Exposed to scams: What beliefs about the world are



associated with fraud victimization? FINRA Investor Education Foundation.

[https://bbbmarketplacetrust.org/wp-content/uploads/2025/07/Foundation\\_Research\\_Brief\\_Exposed\\_to\\_Scams.pdf](https://bbbmarketplacetrust.org/wp-content/uploads/2025/07/Foundation_Research_Brief_Exposed_to_Scams.pdf)

Denburg, N. L. (2010). Why so many seniors get swindled: Brain anomalies and poor decision-making in older adults (L. Harshman, Contributor). In D. Gordon (Ed.), *Cerebrum 2010: Emerging ideas in brain science* (pp. 123–131). Dana Press. [\[Why so man...cision ...\]](#)

Fenton, L., Han, SD, DiGuseppi CG, et al. (2023). Mild cognitive impairment is associated with poorer everyday decision making. *Journal of Alzheimer's Disease*, 94: 1607-1615.

Johnson, D. (2022). *A look at compassion fatigue and resources for social workers*. Practice Perspectives, Fall 2022. National Association of Social Workers.

Lee, J. H., Sutin, A. R., Hajek, A., Karakose, S., Aschwanden, D., O'Súilleabháin, P. S., ... & Luchetti, M. (2025). Loneliness and cognition in older adults: A meta-analysis of harmonized studies from the United States, England, India, China, South Africa, Mexico, and Chile. *Psychological Medicine*, 55, e58.

Leslie DeMarco, 2025, "Mental Health and Financial Exploitation: A Hidden Link" [PPT] NAPSA Conference 2025.

Lindquist, L. A., Miller-Winder, A. P., Schierer, A., Murawski, A., Opsasnick, L., Curtis, L. M., ... & Ramirez-Zohfeld, V. (2022). Aspects of cognition that impact aging-in-place and long-term care planning. *Journal of the American Geriatrics Society*, 70(9), 2646-2652.

Maher, C. A., & Hayes, B. E. (2024). Nonfinancial consequences of identity theft revisited: Examining the association of out-of-pocket losses with physical or emotional distress and behavioral health. *Criminal Justice and Behavior*, 51(3), 459-481.

Samanez-Larkin, G. R., & Knutson, B. (2015). Decision making in the ageing brain: Changes in affective and motivational circuits. *Nature Reviews Neuroscience*, 16(5), 278–289.

Spreng, N., Karlawish, J., & Marson, D. (2016). Cognitive, social, and neural determinants of diminished decision-making and financial exploitation risk in aging and dementia: A review and new model. *Journal of Elder Abuse & Neglect*, 28(4–5), 320–334.

OUR WHY: **REVOLUTIONIZE  
THE WAY PEOPLE  
WORK TO ENSURE  
THE WORLD IS A  
HEALTHIER PLACE.**



[theacademy.sdsu.edu](http://theacademy.sdsu.edu)

6505 Alvarado Road, Suite 107; San Diego, CA 92120 (619) 594-3546