

# Addressing Fraud and Scams in APS Service Plans

INSTRUCTOR LED TRAINING

PARTICIPANT 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.

## Introduction

We are pleased to welcome you to **Addressing Fraud and Scams in APS Service Plans, Participant 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) Education Committee
- 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)

## 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 workers 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

## Table of Contents

Funding Sources.....	1
Introduction.....	2
Partner Organizations.....	3
Acknowledgements.....	4
Table of Contents.....	5
Executive Summary.....	6
Course Outline.....	7
Handout: Fraud Recovery Resource Mapping Worksheet.....	20
Handout: Fraud Recovery Service Planning.....	25
Handout: Case Scenarios.....	29
Appendix: Resource Handout.....	34
References.....	36

## 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>





## Addressing Fraud and Scams in APS Service Plans



Instructor-Led Training


We create experiences that transform the heart, mind, and practice.

### 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

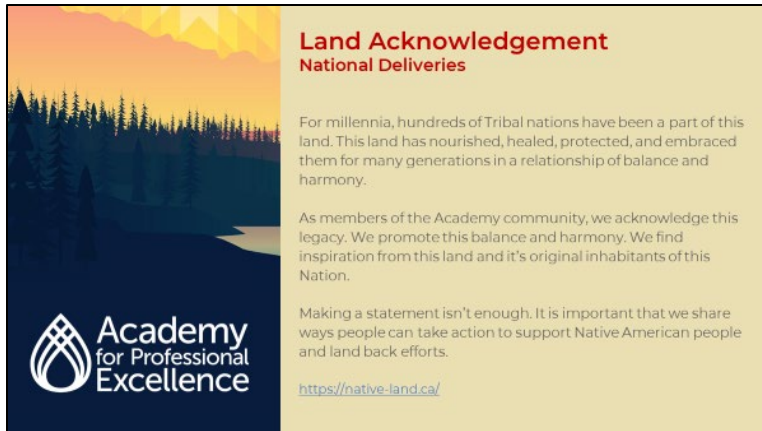



### Purpose of Land Acknowledgement



The purpose of a land acknowledgement is to recognize the relationship of indigenous peoples to the land. It is multi-faceted in its meaning. It shows respect to the people of the land, to the land itself and to their relationship to one another. They are statements that recognize the dispossession from the land, the harm brought by colonial practices, beliefs and policies. They validate and recognize the continued presence of indigenous peoples everywhere. Lastly, when offered in earnest and with sincerity, they are the first steps in reconciliation and healing.

The slide features a background image of a forest at sunset. The Academy for Professional Excellence logo is in the bottom left. The title "Land Acknowledgement National Deliveries" is in red. The text discusses the history of Tribal nations and the Academy's commitment to land back efforts.

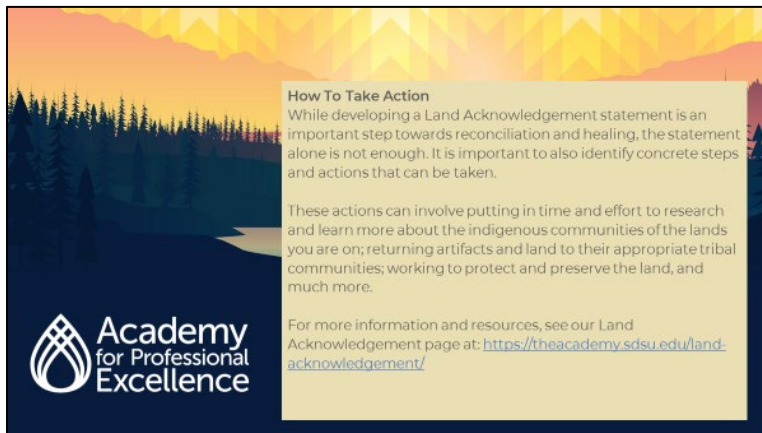
**Land Acknowledgement  
National Deliveries**

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 and it's original inhabitants of this Nation.

Making a statement isn't enough. It is important that we share ways people can take action to support Native American people and land back efforts.

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

The slide features a background image of a forest at sunset. The Academy for Professional Excellence logo is in the bottom left. The title "How To Take Action" is in bold. The text explains the importance of concrete steps and provides a link to the Land Acknowledgement page.

**How To Take Action**

While developing a Land Acknowledgement statement is an important step towards reconciliation and healing, the statement alone is not enough. It is important to also identify concrete steps and actions that can be taken.

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.

For more information and resources, see our Land Acknowledgement page at: <https://theacademy.sdsu.edu/land-acknowledgement/>

The slide has a white background with a large orange geometric design on the right. The title "Housekeeping" is in orange. Below it are three items: "Technology" with a laptop icon, "Agenda" with a document icon, and "Agreements" with a handshake icon.

**Housekeeping**

-  **Technology**
-  **Agenda**
-  **Agreements**



### 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.

### Introduction to “Fraud” and “Scams”

**FRAUD ALERT**

Legal term for deception used to gain money or resources



Informal term for deceptive schemes

**LANGUAGE**

Language shapes how clients understand and respond to fraud

### At the Watercooler Chat



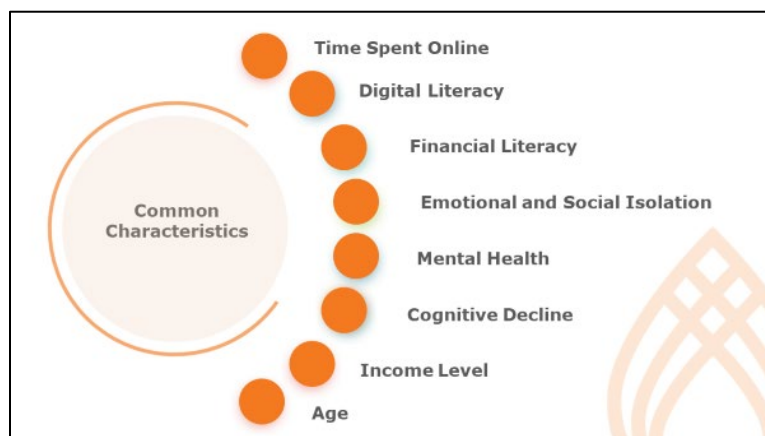
*Think of a recent scam or fraud you have witnessed or heard about from clients.*

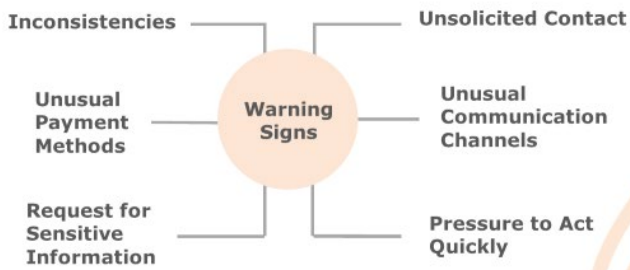
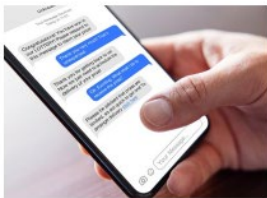
## Fraud and Manipulation

### SOCIAL ENGINEERING

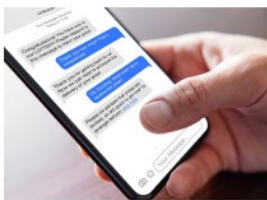
Manipulating people  
into giving up  
information or access

- 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?



**Warning Signs of Fraud Victimization****Fraud Type: Phone Scams – How They Work**

- Unsolicited calls
- Personal info used
- Fabricated emergencies
- Government impersonation
- Charity appeals
- Tech support ruse
- Landline reliance
- Trust in authority
- Cognitive/social vulnerability

**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



**Fraud Type: Emergency Scams – How They Work**

- “Grandchild in trouble” calls
- Fake arrests or medical emergencies
- Scammer poses as relative or official
- AI-generated voices or videos
- Courier pickup or wire transfers
- Personal info pulled from social media

**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”

**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

**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

**Fraud Type: Romance Scams – How They Work**

- Start on social media or dating apps
- Scammer poses as military officer or businessperson
- Use stolen photos & fake profiles
- Gradual emotional grooming
- Shared stories & flattery
- Crisis introduced (money needed)
- Escalating financial requests
- Threats or emotional blackmail if victim hesitates

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

- Rapid emotional bonding
- Requests for money tied to emergencies
- Avoidance of video calls or meetings
- Payment via cards or crypto
- Emotional blackmail or threats

**Fraud Type: Investment Fraud – How They Work**

- Start with unsolicited contact
- Often linked to romance scams
- “Insider” crypto or trading tips
- Fake dashboards show growth
- Victim encouraged to invest more
- Withdrawal blocked by fake fees
- Payment via crypto, wire, or gift cards
- Exploit hope, trust, and fear

**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

**Consequences of Fraud: Word Cloud**

When you hear the phrase, “financial harm from fraud,” what words or images come to mind?

**Consequences of Fraud: Financial Harm**

- Financial loss
- Ongoing financial harm through identity theft
- Cost of recovery
- Impact on financial stability and service planning

**Consequences of Fraud: Emotional Harm**

**Waterfall  
Chat**

- 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

**Consequences of Fraud: Health and Social**

- Stress harms the body
- Mental health toll
- Isolation deepens risk
- Fear of losing autonomy
- Daily life disrupted

## Handout: Fraud Recovery Resource Mapping Worksheet

[illegible]

### Resource Mapping

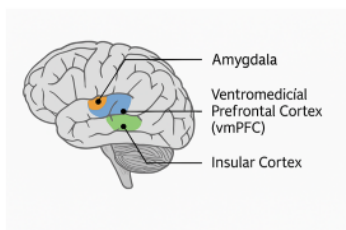


### Correlation Between Fraud and the Brain



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

### Changes in Neurocognition and Decision-Making



- Amygdala:**
- Processes emotional salience
  - ↓ negative cues & ↑ positive cues
- vmPFC:**
- Integrates emotional signals into decision-making
  - ↓ Ability to stop when something feels wrong
- Insular Cortex:**
- Interrupts bodily signals
  - ↓ intuitive awareness of danger

### How Brain Changes Impact Scam Susceptibility



- Frontal lobe aging → reduced executive function
- Difficulty weighing long-term vs. short-term outcomes
- Avoidance/delegation of financial or healthcare decisions
- Neurochemical shifts → altered risk perception and impulse control

### Brain Region Match-Up Activity



### Additional Cognitive Vulnerabilities



- Loneliness linked to cognitive decline
- Isolation → elevated stress hormones (e.g., cortisol)
- Cortisol may damage frontal cortex (decision-making)
- Early signs: missed bills, poor judgment, unusual purchases
- Financial missteps may precede cognitive diagnosis

### Loneliness and Fraud Susceptibility



- Loneliness activates the brain's threat response system
- Reduces judgment, increases emotional reactivity
- Linked to cognitive decline and scam susceptibility
- Scammers target emotional needs

**APS role:** assess isolation, explore online behavior, normalize experience

### 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?


### 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




### 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
- 


### 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



### Introduction to Service Planning

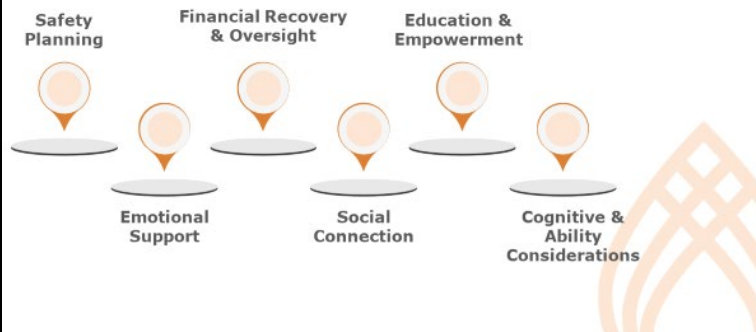
Person-Directed	Trauma-Informed	Culturally Responsive
Client-led goals	Emotional safety	Respect values and beliefs
Strengths-based	Avoid re-traumatization	Language access
Risk tolerance	Empowerment	Cultural Humility
Flexible planning	Normalize experience	Inclusive Communication



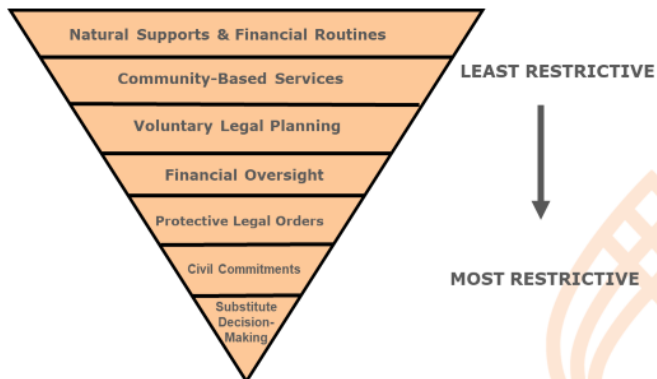
## Handout: Fraud Recovery Service Planning

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>

### Fraud Recovery Service Planning

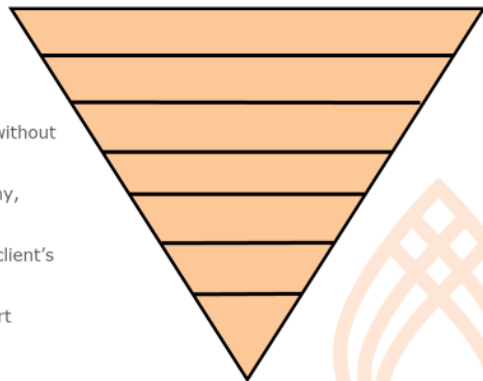


### The Scams Inverted Intervention Triangle



### Harm Reduction

- Reduce impact, even if contact continues
- Support safer choices without judgment
- Focus: safety, autonomy, future change
- Tailor interventions to client's strengths and risks
- Collaborate with support networks



### Cognitive and Behavioral Strategies



### 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

### 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

**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?

**Applying these Skills to Fraud Cases**

Read and review the case scenario



- What are the key concerns?
- 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?



Participate in discussion and reflection

## 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?*

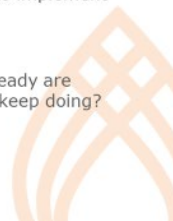


**Review and Summary**

- 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

**P-I-E**

- **P**riceless piece of information
  - What has been the most important piece of information to you today?
- **I**tem to implement
  - What is something you intend to implement from our time together today?
- **E**ncouragement you received
  - What is something that you already are doing and were encouraged to keep doing?



### Evaluations


Your feedback is valuable!

- Please complete evaluations.

Thank you for taking time out to spend on your own professional development.

Thank you for what you do for our communities!






Academy  
for Professional  
Excellence

# Thank You!

We envision a world where  
the quality of life for individuals, organizations, and communities  
is transformed into a healthier place.



APSWI  
Adult Protective Services  
Workforce Innovations





## 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.

This page is intentionally left blank.

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