



An International
Association of Technology
& Computer User Groups
Wednesday Workshop

AI SUMMARY
September 23, 2026
Spotting and Stopping
Elder Financial Exploitation
Exploitation Exploitation, Vice President of Consumer Education
American Bankers Association

ATTENDEE TO-DO LIST

- Consider freezing their credit with TransUnion, Equifax, and Experian as a preventive measure against fraud.
- Set up a trusted contact with their bank or financial institution for added protection against financial exploitation. The contact does not need access to the account.
- Enable multi-factor authentication (MFA) for email, banking, and other important accounts.
- Keep devices updated, including enabling automatic updates for Windows, browsers, and applications.
- Use a modern security suite and avoid pirated or cracked software.
- Back up important data, with at least one copy stored offline or isolated.
- If scammed, stop communication with the scammer, contact financial institutions, freeze credit, and report the scam to law enforcement and IC3.gov.

Elder Financial Exploitation Workshop

Sam KunJukunju, VP of Consumer Education at the American Bankers Association Foundation, presented on elder financial exploitation at this Wednesday Workshop. He explained that elder financial exploitation includes both elder theft (by trusted individuals) and elder scams (by strangers), noting that the growing population of older Americans with significant financial resources makes them attractive targets for criminals. Sam highlighted that the Federal Trade Commission estimates older adults lost \$81.5 billion to fraud in 2024, though experts believe this captures only a small proportion of actual incidents, with many cases going unreported.

Elder Financial Exploitation Trends

Sam discussed the increasing prevalence of elder financial exploitation, highlighting how scammers use technology like AI and voice cloning to create urgency and impersonate loved ones or trusted organizations. He explained that while anyone can be targeted, physical, cognitive, and social changes can increase vulnerability, with statistics showing that 40% of older adults live with a disability and one in three older people dies with dementia. Sam outlined two major types of perpetrators: known individuals in the victim's inner circle and unknown scammers often tied to international crime syndicates, before beginning to detail common scams targeting older people, including lottery/giveaway scams and family imposter scams.

Scam Prevention and Protection Tips

Sam discussed various types of scams, including law enforcement impersonation scams, charity scams, romance scams, investment scams, cryptocurrency confidence scams, contractor scams, and tech support scams. He provided specific advice for each type, such as verifying charities through Charity Navigator or Charity Watch, never sending money to someone you haven't met in person, researching investments and brokers using the FINRA broker check tool, and avoiding payment methods like gift cards for tech support issues. Sam emphasized the importance of talking to trusted

contacts about financial decisions and using credit cards for contractor work to enable chargebacks if needed.

Common Scams Targeting Older Adults

Sam presented information about common scams targeting older adults, highlighting that investment scams, tech support scams, and romance scams caused the greatest financial losses in 2025. He explained how artificial intelligence is making scams more effective by enabling deepfake media and voice cloning but emphasized that the best defenses remain the same: verifying requests independently and contacting people through known, legitimate methods. Sam also outlined six protective mechanisms, including slowing down and making security a habit, being mindful of online posts, and being cautious about unexpected communications.

Scam Prevention Strategies Presentation

Sam presented strategies for protecting against scams, emphasizing the importance of verifying requests independently, using strong passwords and multi-factor authentication, and designating trusted contacts to provide a second opinion before sharing personal information or responding to urgent requests. He shared findings from a study showing that avoiding scams isn't about being tech-savvy; it's about recognizing common scam tactics and trusting your instincts. Sam also outlined steps to take if scammed, including stopping communication with the scammer, contacting financial institutions, freezing credit, reporting to law enforcement, and sharing experiences to help others avoid similar situations.

Financial Scam Detection Training

Sam discussed banker training on detecting scams, fraud, and financial exploitation through the ABA, and shared a broker check tool to verify the legitimacy of financial advisors. Judy asked about using the tool outside the US, to which Sam responded that it likely wouldn't work in Canada due to different jurisdiction. Bob shared a personal story about his 92-year-old cousin being scammed out of \$880,000 through a fake inheritance scheme, emphasizing that scammers often tell victims not to inform family members as a manipulation tactic.