CONVERSATIONS FOR CAREGIVERS

Identity Theft Risks for Seniors and Medically Vulnerable Adults

July 22, 2026
12pm - 1pm EST

LEGAL RESOURCES®

SESSION NOTES

Below is a summary of the topics and items discussed on the July 22, 2026 session of **Conversations for Caregivers: Identity Theft Risks for Seniors and Medically Vulnerable Adults**.

SESSION TOPICS

Scope of Problem | Why Seniors Targeted | Warning Signs | Identity Theft Types | Anatomy of Scams
Digital Safety | Legal Protection Tools | Immediate Action Steps | Where to Report

Click Here to Access Recorded Session →

SCOPE OF PROBLEM

- In 2024, 147,127 victims aged 60+ reported $4.8 billion in losses, a 41% jump over the prior year (figures as presented by the speaker) — and reported cases are only part of the true total
- Criminals target seniors strategically: more trusting, more savings, often own real estate and good credit, and less likely to report fraud

WHY SENIORS ARE TARGETED

- Added vulnerability comes from social isolation, cognitive decline, reliance on caregivers, and frequent contact with benefit programs
- Fraudsters tailor pitches to these vulnerabilities and especially target early-stage dementia — making caregivers the first, and sometimes only, line of defense

WARNING SIGNS

- Forgetting recent conversations, repeating stories, missed bill payments, and trouble understanding financial statements
- Increased trust of strangers, giving money to unfamiliar people, unusual online activity, and secrecy about finances — one sign is rarely the issue, but several together is a real red flag

IDENTITY THEFT TYPES

- Seniors are especially exposed to medical identity theft and Medicare fraud, plus IRS/Social Security and estate identity theft
- Medical profiles are high-value — up to $1,000 on the dark web (vs. ~$1 for an SSN, $5–$30 for a credit card) — and are used for prescriptions, false claims, and services, leaving corrupted records and damaged credit
- Watch for bills or debt collectors for services never received, unknown charges on a credit report, and EOBs or Medicare notices listing unfamiliar providers; stolen Medicare numbers can also delay a beneficiary's legitimate claims for months

ANATOMY OF SCAMS

- The "Four P's": **Pretend** (posing as a legitimate agency), **Prize or Problem**, **Pressure** (urgency or fear), and **Payment** (usually cash, gift cards, wire, or crypto) — all four together is almost certainly fraud
- The government won't call you; if your bank calls, hang up, look up the number independently, and call back to verify

Coming Up Next Month

The Sandwich Generation: Caring for Kids and Aging Parents at the Same Time

August 26, 2026
12pm - 1pm EST

Register at www.LRseminars.com

DIGITAL SAFETY

- Use strong, unique passwords and two-factor authentication; avoid links in unsolicited emails or texts; reach benefit sites by typing the address directly
- Legitimate SSA emails always end in ".gov" — check the actual sender address, not the display name
- Document logins (email, banking, credit, Medicare/insurance, pharmacy, social media, phone, cloud) before they're forgotten and review quarterly; lost device passcodes after cognitive decline can be unrecoverable

LEGAL PROTECTION TOOLS

- A durable power of attorney lets a chosen agent manage bills, investments, property, and Medicaid applications once the person no longer can — best set up before a crisis, while the person can still direct their wishes
- POA is powerful but not instant; expect to resubmit and follow up, especially with healthcare providers

IMMEDIATE ACTION STEPS

- Review Medicare notices and statements monthly; set up banking and credit alerts (a daily balance text flags problems fast)
- Place a free credit freeze at all three bureaus (Equifax, Experian, TransUnion), add a trusted-contact designation, and build a relationship with the local branch
- Screen and background-check in-home care providers, and get financial details in writing before any transaction

WHERE TO REPORT

- FTC (ReportFraud.ftc.gov), the FBI's IC3, Medicare fraud, and SSA scam reporting
- AARP Fraud Watch Helpline and your state's Adult Protective Services (APS)

Q&A HIGHLIGHTS

Q1: Is it helpful to load a program like Guardio on a parent's device to alert them to fraud?

A: These tools can help — many block phishing and malicious links, and newer phones increasingly auto-flag scam texts — so read reviews before choosing. The stronger habit is coaching your care recipient not to share information or feel obligated to respond, and to run anything questionable past a trusted person.

Q2: Is there an equivalent to a credit report for checking Medicare claims?

A: Set up an online account for the Medicare plan or supplement and review it regularly. You can see medications, hospital and rehab charges, and which providers billed — which is how you catch problems, like a provider listed for a visit that never happened. Monitor it and advocate when something looks wrong.

Q3: Any advice for when exploitation comes from inside the family or a caregiver — like large loans the person can't remember taking?

A: It's hard to detect and unfortunately common with family, roommates, and close contacts. The best defense is frequent, open conversation about scams and people taking advantage. With cognitive decline, don't hesitate to call Adult Protective Services, and talk to an attorney about whether it's time to petition for guardianship or conservatorship.

Q4: My parent is in early dementia and gets suspicious when I raise power of attorney. How do I get around this?
A: Pushing hard tends to backfire. Keep returning to the conversation over time, framed positively: the POA is there to help them, with you as a partner rather than taking over. It's especially hard for someone giving up a business or long-held independence, so patience and consistency matter more than any single talk.

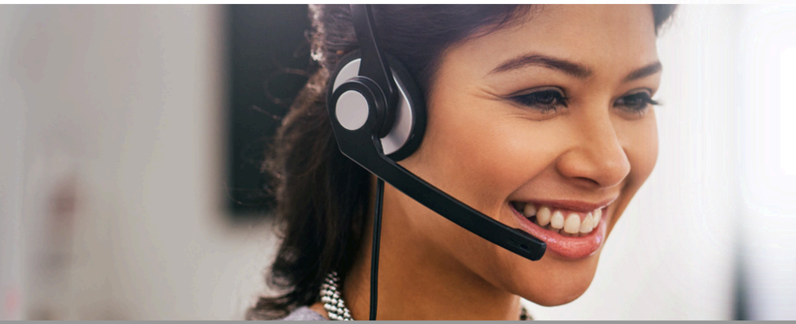
Q5: Even with a credit freeze, new accounts still got opened. Can that be prevented entirely?
A: Larger lenders honor a freeze; some high-interest personal-loan operations may claim not to see it. Know the two tools: a fraud alertis set with one bureau and shared with the other two, prompting extra identity checks. A credit freeze fully cloaks your profile but must be set individually with all three bureaus (Equifax, Experian, TransUnion) — if a lender checks only the one you missed, the freeze won't stop it.

ABOUT OUR SPEAKER:

TERRI PROCTOR | STOP ELDERLY SCAMS

Terri Proctor founded Stop Elderly Scams in 2023, after her elderly mother was drawn into multiple romance scams over four years and lost more than $150,000. Drawing on her firsthand experience as her mother's caregiver — navigating cognitive decline, powers of attorney, and financial and medical monitoring — Terri shares stories and guidance to help other caregivers recognize and prevent elder fraud. She also produces a monthly video series with a cybersecurity expert on how AI is reshaping scams.

DISCLAIMER: This summary highlights key webinar points and questions. For comprehensive details, view the full seminar at **LRSeminars.com.**



Contact Us

Our Member Services team is available for assistance.

Phone: 800.728.5768
Email: info@legalresources.com

www.legalresources.com