

CONVERSATIONS FOR CAREGIVERS

Fund Recovery from Identity Theft and Fraud

November 26, 2025
12pm - 1pm

SESSION NOTES

Below is a summary of the topics and items discussed in the Conversations for Caregivers session on **Fund Recovery from Identity Theft and Fraud**.

These notes were compiled following a virtual webinar presentation and are provided for general informational purposes only. The session was presented by an attorney licensed in a specific state. Attorneys are not licensed in every state, and laws, regulations, terminology, and requirements vary by jurisdiction. This content is not legal advice and should not be relied upon as such. While best efforts were made to accurately capture the discussion, this document is a transcription summary and may contain errors, omissions, or inaccuracies in wording, facts, or interpretation. Legal Resources and the presenter are not responsible or liable for any consequences that may arise from reading, using, or interpreting this material. For legal advice specific to your situation, please consult with a qualified attorney licensed in your state.

SESSION TOPICS

Elder Fraud Statistics | Recovery Framework | Immediate Response Steps | Documentation Requirements | Government Reporting | Financial Institution Disputes | Caregiver Considerations | Long-Term Protection

[Click Here to Access Recorded Session](#) →

ELDER FRAUD REALITY

- People over 60 lose tens of billions of dollars annually to fraud schemes
- In 2024, crypto-related fraud alone accounted for \$9.3 billion in losses among American adults
- Elderly victims lose more money than younger generations due to accumulated wealth
- Romance scams and cryptocurrency scams are currently surging and causing significant financial damage

RECOVERY FRAMEWORK

- **Step 1 - Identify Exploitation:** Notice suspicious signs like unauthorized charges, missing funds, or unexpected creditor contacts
- **Step 2 - Report to Authorities:** Contact appropriate agencies to place holds on fraudulent accounts and initiate investigations
- **Step 3 - Investigation Phase:** Institutions contact merchants, determine responsibility, and gather evidence
- **Step 4 - Fund Return:** The goal of early action is recovering stolen funds to the victim
- Time is critical — the earlier you act, the higher the chances of successful recovery

IMMEDIATE RESPONSE STEPS

- Contact financial institutions immediately to report unauthorized charges and freeze affected accounts
- Notify all three credit bureaus (Equifax, Experian, TransUnion) to place protection
- Fraud alerts require notifying only one agency, which then alerts the others
- Credit freezes must be placed with each bureau individually and require PIN numbers to unlock
- Update all passwords and enable two-factor authentication on sensitive accounts
- Set up transaction monitoring alerts for large withdrawals or transfers

DOCUMENTATION ESSENTIALS

- Create a dedicated recovery file containing all theft-related documentation
- Keep copies of all correspondence, phone call details, dates, names, and reference numbers
- Save bank and credit card statements showing fraudulent charges
- Preserve emails, text messages, and screenshots of communications with scammers
- Maintain records of payments made to fraudsters and a timeline of events
- Documentation may be needed indefinitely for future disputes or investigations

GOVERNMENT AGENCY REPORTING

- **Federal Trade Commission (FTC):** File complaint at identitytheft.gov to receive personalized recovery plan; FTC complaints can serve as police reports for financial institutions
- **FBI IC3:** Report internet-enabled crimes; their Recovery Asset Team has frozen over \$561 million with a 66% success rate
- **IRS:** File Form 14039 for tax fraud; create online account for change notifications; request Identity Protection PIN number
- **Local Police:** File police report or incident report for documentation purposes; use non-emergency number, not 911



WORKING WITH BANKS

- Contact fraud department immediately upon discovering unauthorized activity
- First action will be closing the fraudulent account before investigation begins
- Request written confirmation that fraudulent accounts are closed
- Complete any required claim forms in a timely manner
- Investigations typically take 1-2 weeks depending on the institution
- Follow up regularly and respond promptly to requests for additional information
- Each financial institution has different procedures — ask about their specific process

CAREGIVER CONSIDERATIONS

- Legal authority is essential — power of attorney, guardianship, or conservatorship may be required
- Credit bureaus and some financial institutions refuse to work with third parties regardless of documentation
- Power of attorney must be properly executed, often requiring notarization
- Be mindful of HIPAA and privacy laws when accessing medical or financial information
- Cognitive impairment assessments determine whether guardianship appointment is necessary
- Build preventive networks through partnerships with local organizations, law enforcement, and healthcare providers

LONG-TERM PROTECTION

- Request free credit reports regularly from annualcreditreport.com (now available weekly)
- Create accounts with credit bureaus, IRS, Social Security Administration, and USPS for monitoring
- USPS Informed Delivery provides email previews of incoming mail to detect theft
- Review financial statements monthly to catch unauthorized activity early
- Consider extended fraud alerts (7 years) or credit freezes for severe cases
- Enroll in identity theft protection services for additional monitoring
- Provide emotional support — victims often experience shame; remind them fraud happens to anyone

KEY TAKEAWAYS

1. Time is everything — the faster you act after discovering fraud, the higher your recovery chances
2. Documentation is crucial and should be maintained indefinitely for potential future disputes
3. Legal authority (power of attorney or guardianship) is essential for caregivers to act on behalf of care recipients
4. Create accounts with government agencies and credit bureaus before fraudsters do
5. The FTC complaint can serve as a police report and provides a personalized recovery plan
6. Follow up regularly with financial institutions — you must advocate for the victim throughout the process

Q&A HIGHLIGHTS

Q1. What is the IRS PIN number mentioned for tax protection, and how does it work?

A: The IRS offers an Identity Protection PIN — a 6-digit number required for your tax return to be accepted. You request it through the IRS website, and they mail it to you before each tax season. Without the correct PIN, tax returns filed under that Social Security number are automatically rejected, preventing fraudulent filings. This protection is available to anyone, not just previous fraud victims. Creating an IRS online account also provides notifications of any changes to your tax information.

Q2. Is it free to create monitoring accounts with government agencies and credit bureaus?

A: Yes, all accounts with government and federal agencies are completely free. This includes accounts with the three credit bureaus, the IRS, Social Security Administration, and U.S. Postal Service. These accounts are your right as a citizen and provide the best way to receive notifications about changes to your information. The IRS portal even shows you all notices being mailed to you, helping verify legitimate correspondence.

Q3. What is the best first step if a parent has cognitive impairment, is making bad financial decisions, and you don't have legal authority?

A: The first step is consulting with an attorney who practices guardianship, specifically contested guardianship. When someone is cognitively impaired, they cannot legally grant power of attorney because they lack the capacity to give power. An attorney cannot ethically draft such documents. The necessary path is pursuing guardianship and conservatorship through the courts. A medical assessment confirming the cognitive impairment from their doctor can support this process.

Q4. Does creating a family trust help prevent these types of fraud and provide more protection for large assets?

A: Trusts add security layers since they typically require different approvals before assets can be moved. However, a trust must be properly funded — assets must actually be titled with the trust as owner, which many people neglect. While trusts aren't fail-proof against scams (the administrator is still human and could be deceived), they do create additional barriers. Consult with an attorney about whether a trust structure suits your specific situation and protection needs.

Q5. What steps should we take if my parent cannot recall their IRS PIN?

A: If discovered early in tax season, contact the IRS and they will mail a new PIN number. If your parent can get online, they can verify their information on the IRS website to retrieve the current year's PIN immediately. If time doesn't allow for receiving a new PIN before the filing deadline, submit the tax return anyway — it will be rejected, but if no other fraudulent filing exists, the IRS will accept it. The IRS website provides specific guidance for lost PIN situations.

ABOUT OUR SPEAKER:



Sewitt Estiphanos | Iris Identity Protection

Sewitt Estiphanos works at Iris Powered by Generali, providing identity theft protection services for Legal Resources members. Her current role focuses on quality assurance and training. She began as a certified resolution specialist helping victims of identity theft, giving her firsthand experience understanding the challenges victims face and what it takes to guide them through recovery. She has worked extensively with older adults impacted by fraud and identity theft.



Mohamed Diabagate | Iris Identity Protection

Mohamad Diabagate has been with Iris for an extended period, working his way through various positions within the company. Starting from ground-level roles, he has gained comprehensive knowledge of all steps in the identity theft resolution process. His experience enables him to advise people with confidence about fraud recovery procedures and identity protection strategies.

DISCLAIMER: This summary highlights key webinar points and questions. For comprehensive details, view the full seminar at [LRSeminars.com](https://www.LRSeminars.com).

Contact Us

Our Member Services team is available for assistance.

Phone: 800.728.5768

Email: info@legalresources.com

www.legalresources.com