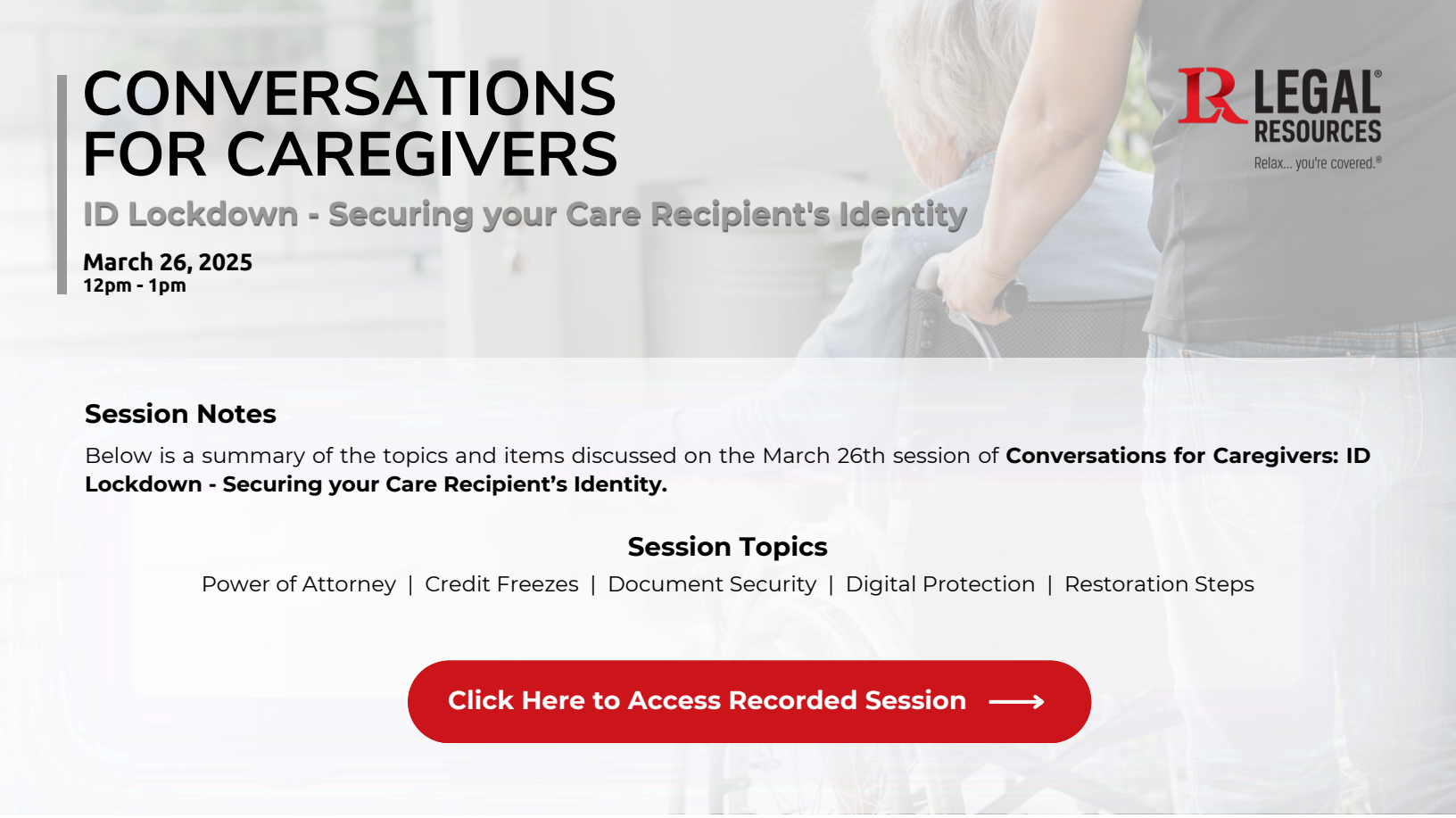
CONVERSATIONS FOR CAREGIVERS

ID Lockdown - Securing your Care Recipient's Identity

March 26, 2025
12pm - 1pm



LEGAL RESOURCES
Relax... you're covered.®

Session Notes

Below is a summary of the topics and items discussed on the March 26th session of **Conversations for Caregivers: ID Lockdown - Securing your Care Recipient's Identity.**

Session Topics

Power of Attorney | Credit Freezes | Document Security | Digital Protection | Restoration Steps

Click Here to Access Recorded Session ⟶

Power of Attorney: The Essential Foundation

Importance for Caregivers

- Legal Requirement: A power of attorney (POA) document is essential to taking any identity protection or recovery actions on behalf of a care recipient.
- Financial institutions, credit bureaus, and identity theft resolution services will require documentation of legal authority.
- Without POA or a court order, caregivers cannot freeze credit reports, dispute fraudulent accounts, or access financial/medical information on behalf of their care recipients.

Key Features of POA for Identity Protection

- **Scope of Authority:** Can specify different types of decisions (financial, medical, housing) the caregiver is authorized to make.
- **Durable POA:** Ensures authority continues even if the principal becomes incapacitated.
- **Legal Protection:** Enables caregivers to advocate effectively for care recipients who cannot communicate their wishes.
- **Customizable:** Can be drafted to include specific identity protection and recovery language.

Best Practices

- Choose a trustworthy agent with clear roles and responsibilities.
- Consult with an attorney to create a legally sound document with appropriate language.
- Consider having the POA include explicit permission for identity theft prevention and recovery actions
- If the care recipient is resistant, discuss POAs that activate only after specific triggering events

Identity Protection Strategies

Document Security

- Store critical documents (birth certificates, Social Security cards, passports) in locked cabinets or safes.
- Shred sensitive documents containing personal information when no longer needed.
- Limit sharing personal information, even with family members.
- Be cautious about what information caregivers and service providers can access.

Financial Account Monitoring

- Regularly check bank statements and credit card activity for suspicious transactions.
- Set up alerts for transactions over a certain amount.
- Consider view-only access for caregivers to monitor accounts without transaction capabilities.
- Look for small unauthorized charges that may precede larger fraud attempts.

Medical Record Security

- Review medical bills and explanation of benefits for treatments not received.
- Control access to medical records through proper authorization.
- Be alert for unfamiliar medical bills, which may indicate medical identity theft.

Digital Security

- Use strong, unique passwords for all online accounts.
- Enable two-factor authentication whenever available.
- Limit online footprint and remove personal information from people-search websites.
- Be cautious about social media sharing (avoid posting birthdays, addresses, or travel plans).
- Use spam-blocking apps from mobile providers and register for the FTC's Do Not Call registry.

Government Account Monitoring

- Create a Social Security Administration account to monitor benefits.
- Get an IRS PIN to prevent fraudulent tax filings.
- Be aware that government agencies (like Social Security) will never call, text, or email you.

Responding to Identity Theft

Warning Signs

- Unexpected bills or debt collection calls.
- Missing financial statements or credit cards.
- Unusual account activity or unfamiliar withdrawals.
- Receiving medical bills for services not provided.

Immediate Steps

1. **Contact Financial Institutions:** Notify banks or credit card companies about suspicious activity.
2. **Place Fraud Alerts/Credit Freezes:** Add protection to credit reports (freezes provide stronger protection than alerts).
3. **File Police Report:** Create documentation needed for disputing fraudulent accounts.
4. **Contact Credit Bureaus:** Each bureau must be contacted individually for credit freezes.
5. **Report to FTC:** Visit identitytheft.gov for a recovery plan and reporting resources.

Fraud Alert vs. Credit Freeze

- **Fraud Alert:** Statement on credit report requiring additional verification before opening new accounts (lasts 1 year or 7 years).
- **Credit Freeze:** Completely blocks access to credit report until lifted with a PIN; must be placed with each bureau individually.
- Freezes provide stronger protection but require advance planning when legitimate credit is needed.

Special Considerations for Caregivers

Third-Party Oversight

- Conduct background checks on potential caregivers, especially non-family members.
- Create clear contracts outlining responsibilities and limitations regarding personal information.
- Maintain regular communication and monitor caregiver activities.
- Consider having multiple family members involved in oversight.

Balancing Access and Protection

- Determine appropriate levels of information sharing based on trust and necessity.
- Set clear boundaries regarding mail handling, financial document access, and online account usage.
- Discuss expectations about privacy and confidentiality with all parties involved in care.

Attendee Questions:

Q1: My mother has dementia, and her sister-in-law asked for her social security number, which my mom gave her. How can I protect my mom?
A: Place credit freezes with all three credit bureaus immediately. This prevents new accounts from being opened in her name, though it won't protect existing accounts. Since you and your brother have power of attorney, you're in a good position to monitor her financial accounts for suspicious activity.

Q2: What are the pros and cons of identity theft insurance?
A: Identity theft insurance primarily covers out-of-pocket expenses during the restoration process, including attorney fees for severe cases, reimbursement for lost work time, and sometimes stolen funds. There are a few drawbacks, though coverage varies between policies. Some policies now include direct reimbursement for stolen funds that banks don't refund.

Q3: If I freeze the credit of my care recipient, will that prevent me from opening accounts in their name?
A: Yes, if the bank requires a credit check. You would need to temporarily lift the freeze, allow the credit check to proceed, and then refreeze it afterward. The bank will also require your power of attorney documentation before opening any account on their behalf.

Q4: What options exist when someone is already incapacitated and can't grant power of attorney?
A: When someone lacks the capacity to consent to power of attorney, the alternative is petitioning for guardianship through the court system. Financial institutions and credit bureaus accept either power of attorney or court orders (like guardianship) for identity protection actions. For complex situations, consult with an attorney who specializes in elder law.

.

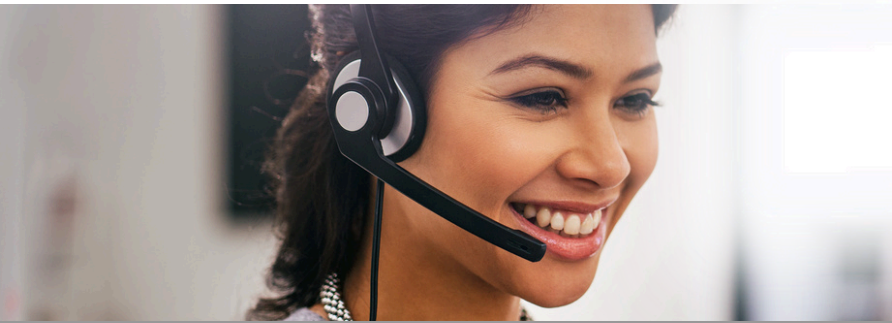
Q5: How can I reduce spam calls and texts to my care recipient's phone?
A: Use carrier-specific apps like T-Mobile's Scam Shield, AT&T Active Armor, or Verizon Call Filter. While no solution blocks 100% of spam (as scammers constantly change numbers), these tools significantly reduce unwanted communications. Use AI technology to establish code words with your care recipient to verify emergency communications against increasingly sophisticated voice scams.

About our speaker: EUGENE NAKOUYE IRIS POWERED BY GENERALI

Eugene Nakouye is the Operations Manager for Iris Identity Protection, with 11 years of dedicated service. Starting as a case manager in the Travel Assistance department, he now oversees the entire case resolution process for identity theft victims, collaborating with law enforcement, financial institutions, and legal teams to help restore identities and secure personal information. Eugene leads a team of specialists, providing ongoing training to maintain high service standards.

Beyond his managerial duties, Eugene educates the public about identity theft prevention through workshops and seminars, sharing expertise on safeguarding personal information, recognizing phishing scams, and understanding cyber threat trends. His goal is to empower individuals and businesses against identity theft. Eugene's credentials include Fair Credit Reporting Act Certification and CompTIA Security+ certification, reflecting his identity protection and information security expertise.

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