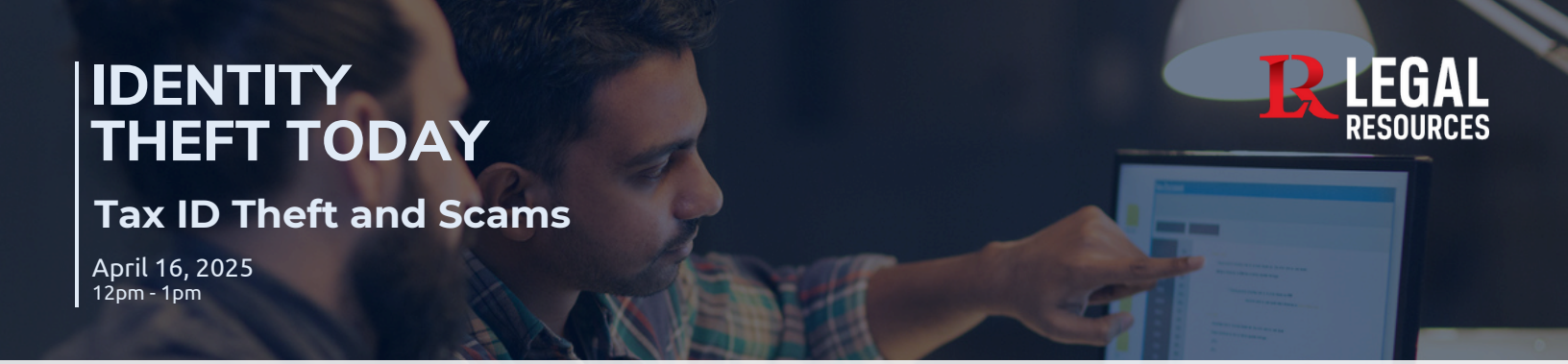


IDENTITY THEFT TODAY

Tax ID Theft and Scams

April 16, 2025
12pm - 1pm

LEGAL RESOURCES

SESSION NOTES

Below is a summary of the topics and items discussed on the April 16, 2025 session of **Identity Theft Today: Tax ID Theft and Scams.**

SESSION TOPICS

Tax Fraud | Employment Fraud | Prevention Tips | Identity PINs | Recovery Steps | Digital Security

Click Here to Access Recorded Session ⟶

Understanding Tax Identity Theft

- Occurs when someone uses your personal information to file taxes
- The perpetrator's goal is typically to fraudulently claim your tax refund
- Can affect you, your children, parents, or dependents
- Long resolution time (potentially up to a year)
- Two major consequences: financial loss and time lost fixing the issue

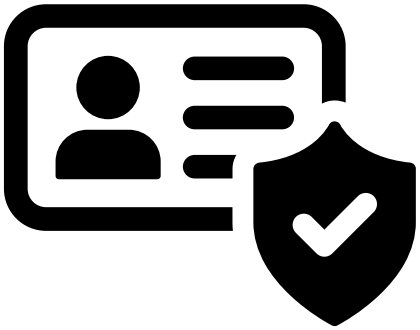
Warning Signs of Tax Identity Theft

Official Document Issues:

- Tax return rejection notices
- Receiving W-2 or 1099 forms from employers you never worked for
- Documents for unemployment benefits you didn't apply for
- Employer identification number (EIN) you didn't apply for

Unexpected Communications:

- Unreported income alerts (CP 2000 series notices)
- Unsolicited offers to help with online accounts
- Notifications about accounts created or accessed without your knowledge



Account Security Alerts:

- Password reset alerts for IRS accounts
- Login verification alerts
- Data breach notifications

Financial Discrepancies:

- Unexpected wages on Social Security account
- Income reported from unknown employers

Prevention Strategies

Filing Practices:

- File taxes as soon as possible after receiving your W-2
- Don't wait until the April 15 deadline
- Consider getting an IRS Identity Protection PIN
  - Available at: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin

Account Security:

- Secure online accounts with complex, unique passwords
- Consider using a password manager for your accounts
- Change passwords at least annually for self-created passwords

Information Protection:

- Safeguard Social Security numbers, usernames, and passwords
- Secure data for dependents and deceased persons
- Properly dispose of sensitive documents (shredding)
- Remove personal information from Google search
  - Available at: https://support.google.com/websearch/answer/9673730

Monitoring Activities:

- Review credit reports monthly (annualcreditreport.com)
- Monitor bank statements regularly for suspicious transactions
- Check Social Security account for unexpected wages

Communication Safety:

- Be cautious when providing personal information
- Never give personal information to unexpected callers
- Remember IRS communication is primarily through mail, not phone or text

Response to Identity Theft

- Contact IRS at (800) 908-4490
- File IRS Form 14039 (Identity Theft Affidavit)
- Review credit reports monthly
- Monitor bank statements regularly
- Check Social Security account for unexpected wages
- Get an IP PIN after reporting

Business Identity Theft Concerns

- Similar warning signs: rejected returns, duplicate EIN filings
- Unexpected notices or transcripts
- Letters 6042C or 5263C from IRS
- Missing expected IRS correspondence (due to address changes)

Employment Fraud Connection

- Tax identity theft is often connected to employment fraud
- Employers report income under your SSN
- IRS records show unreported income
- Review Social Security work history at socialsecurity.gov/myaccount
- Consider locking your SSN through E-Verify (everify.gov/my-e-verify)

Resources

- IRS Identity Protection PIN: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin
- Google information removal: https://support.google.com/websearch/answer/9673730
- Annual free credit reports: annualcreditreport.com

Key Advice and Takeaways

1. File your taxes as early as possible to prevent fraudulent filing
2. Secure an IRS Identity Protection PIN for yourself and your dependents
3. Consider using a password manager for complex, unique passwords
4. Monitor your credit report, bank statements, and Social Security account regularly
5. Tax identity theft incidents are increasing year over year
6. Credit freezes are the most effective protection against new account fraud
7. Do not share security PINs with anyone, even family members

Attendee Questions

Q1: How should we handle a debt collector asking for verification of address and other information?

A: When debt collectors request verification, first ask where the debt originated from. Do not provide personal information immediately. Get the collector's information, tell them you'll call back, and then contact the original company that initiated the debt collection—request written documentation from the debt collector listing the amount owed and account number before providing any information.

Q2: Do you recommend using password managers such as Dashlane, Bitwarden, or Nordpass?

A: Password managers are highly recommended, especially for managing multiple online accounts with complex, unique passwords. While there are security concerns, they are generally secure and far better than using simple, reused passwords or constantly resetting forgotten passwords. Most devices now suggest strong passwords, and password managers help you securely store and manage them.

Q3: Can freezing your credit help with tax identity theft?

A: Credit freezes are excellent for preventing the unauthorized opening of new accounts but do not protect against tax identity theft. Freezing your credit blocks access to your credit reports, preventing creditors from issuing new loans or credit cards in your name. However, the IRS does not check credit reports when processing tax returns. The best protection against tax identity theft is an IRS Identity Protection PIN.

Q4: How often should you change your passwords for online accounts?

A: While cybersecurity experts recommend changing passwords every three months, this is impractical for most people with numerous accounts. A reasonable compromise is changing passwords at least once a year for accounts you create yourself. Changing passwords less frequently for system-generated complex passwords stored in a password manager is generally acceptable due to their strength.

Q5: What are the risks when you file a tax extension?

A: The primary risk of filing a tax extension is giving identity thieves more time to file fraudulently in your name. The longer you wait to file, the more you expose yourself to potential tax identity theft. If you need an extension, it's strongly recommended to have an IRS Identity Protection PIN in place to prevent unauthorized filing. Without this protection, you risk lengthy resolution processes and delayed legitimate refunds.

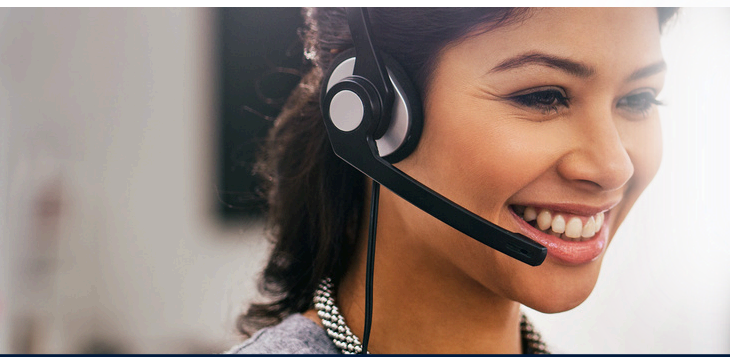
ABOUT OUR SPEAKER:

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