IDENTITY THEFT TODAY

Trending Threats

November 19, 2025
12pm - 1pm

LEGAL RESOURCES

SESSION NOTES

Below is a summary of the topics and items discussed on the November 19, 2025 session of **Identity Theft Today: Trending Threats.**

The information provided in this session recap is for informational purposes only. The content has been summarized and transcribed based on the session and is not a direct representation of the presenters' exact words. The material shared is intended to provide general legal information and is not intended as legal advice. It may not reflect the laws of all jurisdictions. Attendees are encouraged to consult a qualified legal professional in their jurisdiction for advice tailored to their specific circumstances.

SESSION TOPICS

AI Voice Cloning | Investment Scams | Imposter Scams
Online Shopping Fraud | Romance Scams | Cybersecurity Protection

Click Here to Access Recorded Session ⟶

IDENTITY THEFT FUNDAMENTALS

- Credit freezes are essential first-line defense - freeze all three credit bureaus (Equifax, TransUnion, Experian) to prevent unauthorized account openings
- Personal information from 2017 Equifax breach affecting 100+ million Americans remains on dark web, continuously used by scammers
- Identity theft differs from fraud - theft involves stealing personal information, fraud involves monetary losses through deception

AI-POWERED SCAM EVOLUTION

- **Voice Cloning**: Scammers use AI to replicate voices of family members or authority figures with frightening accuracy
- **Family Passwords**: Establish unique passphrases only real family members would know to verify caller identity
- **Urgency Tactics**: AI enables real-time responses making emergency scenarios more believable and harder to detect
- **Deepfake Technology**: Creates convincing videos of celebrities or financial experts promoting fraudulent investment schemes

MAJOR SCAM CATEGORIES

- **Investment/Crypto Scams**: $5.7 billion lost in 2024, primarily through "pig butchering" schemes building fake relationships before financial exploitation
- **Imposter Scams**: Criminals pose as government agents, law enforcement, or bank officials claiming account compromise
- **Romance Scams**: Target lonely individuals through extended emotional manipulation before requesting money
- **Online Shopping Fraud**: 10% of social media ads are fraudulent, using familiar brand names with subtle URL differences

RED FLAG RECOGNITION

- **Authority Pressure**: Government agencies never call demanding immediate payment or threatening arrest
- **Payment Methods**: Requests for gift cards, wire transfers, or cryptocurrency indicate fraud
- **Urgency Creation**: Legitimate organizations allow time for verification - scammers insist on staying on phone
- **Too Good to Be True**: Deep discounts (80% off), unexpected winnings, or easy money opportunities signal scams

Coming Up Next Month

Online Shopping Scams

December 17, 2025
12pm - 1pm

Register at www.LRseminars.com

PROTECTION STRATEGIES

Step 1: Hang up and call back using independently verified numbers from official websites or cards
Step 2: Use password managers for unique, strong passwords on every account
Step 3: Enable multi-factor authentication on all financial and email accounts
Step 4: Install browser protection like Bitdefender Traffic Light to identify malicious websites
Step 5: Report scams to FTC, social media platforms, and financial institutions

HUMAN TRAFFICKING CONNECTION

- Many cryptocurrency scammers are victims themselves, forced to work in scam compounds in Southeast Asia
- Criminal enterprises operate like corporations with HR departments, benefits, and structured operations
- International cooperation recently initiated to address these human trafficking/scam operations
- Awareness and reporting help combat both financial crimes and human exploitation

KEY TAKEAWAYS

1. Freeze credit reports immediately - this single action prevents most identity theft damage
2. Never trust inbound communications - always verify by calling back using known numbers
3. Pause and consult others when pressured - scammers isolate victims to prevent second opinions
4. Use technology defenses: password managers, multi-factor authentication, and browser protection tools
5. Report all incidents - only 10% of victims report, limiting law enforcement's ability to prosecute
6. Educate vulnerable populations - seniors and isolated individuals face highest risk

Q&A HIGHLIGHTS

1. Are criminals able to get around having a family password?

A: Theoretically yes, nothing is foolproof. However, if you create something really hard to guess that only your family would know, it's extremely difficult for scammers to guess. The key is choosing something unique to your family's shared experiences that wouldn't be discoverable through social media or public records. While not impossible to defeat, family passwords remain one of the most effective defenses against AI voice cloning scams.

2. What if the issue is not technically a scam, but actual bank employees committing fraud by opening accounts to hit internal numbers?

A: This happened with Wells Fargo, where millions of unauthorized accounts were opened by employees. If you have evidence of this happening, file a police report immediately and report it to the bank's fraud department, which operates above branch level. Also pull your credit report to check for unauthorized accounts. The fraud department has incentive to investigate as this represents serious liability for the institution.

3. Are password managers vulnerable to breaches, and is it safe to put all passwords in one place?
A: While no system is 100% secure, password managers are considered the safest option by security professionals. They're far more secure than writing passwords down, using spreadsheets, or reusing passwords. LastPass experienced a breach years ago, but the stolen data remained encrypted and unusable. Password manager companies' entire business model depends on maintaining security, giving them huge incentive to protect data with the strongest available encryption.

4. How can you get legitimate organizations with the wrong phone number to stop calling you?
A: Register with the National Do Not Call Registry (must renew every 5 years). Additionally, directly tell callers to stop calling and contact the organization to request removal from their list. For political organizations, you may need to contact them directly as they often have exemptions from Do Not Call regulations. Document requests and escalate to supervisors if calls persist.

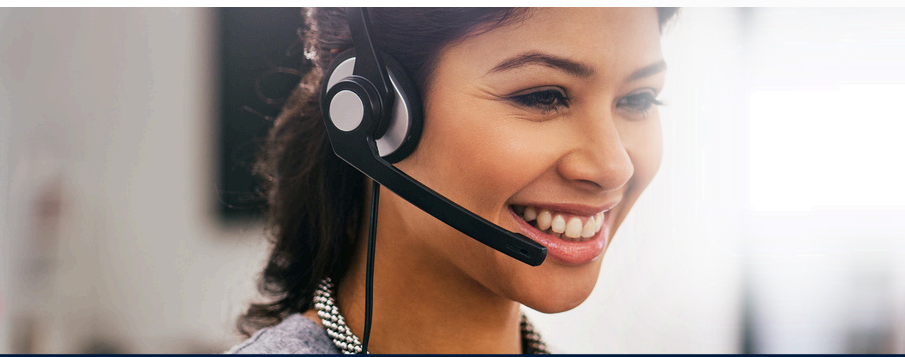
5. How is it possible for scammers to reach so many people and steal billions without more being done at top levels?
A: Scammers operate from countries without extradition agreements (China, Russia, Myanmar), creating safe havens. Technology companies like Meta profit from fraudulent ads ($16 billion annually), preferring to pay fines rather than lose revenue. Government response is slow by design, and creating effective laws takes years. Current political climate further complicates legislative solutions. Until comprehensive privacy laws and international cooperation improve, individuals must protect themselves through education and vigilance.

ABOUT OUR SPEAKERS:

CLIFF STEINHAUER | NATIONAL CYBERSECURITY ALLIANCE

Cliff Steinhauer works for the National Cybersecurity Alliance, a nonprofit organization dedicated to educating the public on online safety. With a background in business and project management, he transitioned to cybersecurity after the COVID-19 pandemic disrupted his travel industry career. He focuses on helping consumers understand that most security incidents result from social engineering rather than technical hacking, emphasizing practical protection strategies for everyday users. His presentations combine technical knowledge with accessible explanations to empower individuals against evolving cyber threats.

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