IDENTITY THEFT TODAY

Young Identities: Protecting Kids from Scams and ID Theft

June 24, 2025
12pm - 1pm

LEGAL RESOURCES

SESSION NOTES

Below is a summary of the topics and items discussed on the June 24, 2025 session of **Identity Theft Today: Young Identities: Protecting Kids from Scams and ID Theft.**

SESSION TOPICS

Social Commerce Scams | Sextortion Prevention | Peer-to-Peer Payment Protection
Scammer Profiles | Child Identity Theft | Recovery Strategies

Click Here to Access Recorded Session →

Scammer Fundamentals

- **Core Scammer Tactics:** All scams follow consistent patterns - manufacturing opportunities, creating crises, or threatening consequences
- **Adaptive Nature:** Scammers follow headlines and current events (COVID vaccines, student loan forgiveness, natural disasters)
- **Technology Savvy:** Early adopters who exploit technological vulnerabilities and manipulate social/emotional cues
- **Organized Crime Element:** Many scams involve organized networks, not lone wolves; some use trafficked "cyber slaves"
- **Aggressive Behavior:** Children need education on recognizing normal vs. aggressive online interactions

Social Media Targeting

- **Prevalence:** 44% of reports involved undeliverable merchandise from social media ads (Facebook, Instagram, TikTok)
- **Target Demographics:** 55% of Gen Z made online purchases while browsing social media; one in three young Americans shop on social media weekly
- **Common Tactics:** Fake product ads with prices "too good to be true" (90% off, $20 AirPods, $40 designer shoes)
- **AI-Enhanced Threats:** Deepfake technology enables impersonation of brands and influencers with fake exclusive deals
- **Direct Messaging Risks:** Reputable companies don't send individual DMs to sell products - always interpret as scams

Payment Scam Prevention

- Peer-to-peer apps (Venmo, Cash App) offer limited fraud protection compared to credit cards
- PayPal provides better reimbursement policies for business transactions versus personal transfers
- Overpayment scams involve sending excess funds then requesting refunds before fraudulent payments are discovered
- Always verify seller reviews and avoid deals shared via direct messages
- Parents should offer to review purchases before children complete transactions

Sextortion Awareness

- **Financial Sextortion Statistics:** 30,000 reports received in 2023 (large increase from previous year)
- **Primary Targets:** Males aged 14-17, though females are also targeted
- **Entry Method:** Development of fake romantic relationships using stolen identities
- **AI Escalation:** Deepfake technology makes video verification unreliable for confirming identity

- Common Process: Immediate request to move off-platform (to WhatsApp, text messaging) to avoid account shutdowns
- Extortion Tactics: Threats to share explicit photos or conversations with friends, family, and school contacts

Coming Up Next Month

Understanding and Using Private Virtual Networks (VPNs)

July 16, 2025
12pm - 1pm

Register at www.LRseminars.com

Child Identity Protection

- Children's identities are valuable because they represent "blank slates" perfect for synthetic identity creation
- Social Security Administration doesn't share children's SSNs with credit bureaus, creating verification gaps
- Why Children Are Targets: Clean credit slate perfect for synthetic identity theft; theft goes undetected longer
- Common Uses: Employment fraud, utility accounts, government benefits, financial accounts
- Warning Signs: Pre-approval credit offers, IRS notices about tax returns, debt collector contact, student loan denials
- Family Member Risk: More severe identity theft (utilities, government benefits) often perpetrated by family members

Protection and Recovery Strategies

- Information Security: Teach children what constitutes personal information (address, birthdate, school, license numbers)
- Credit Monitoring: Establish credit reports and consider credit freezes for children (requires mailed documentation)
- Platform Safety: Verify influencer accounts through official verification badges; avoid deals shared via DM
- Recovery Process: Pull credit reports from all bureaus, dispute incorrect information, handle specific account fraud

Attendee Questions

Q1: Why are children especially vulnerable to identity theft, and how does synthetic identity theft operate?

A: Children are perfect targets because they represent a "blank slate" from a credit standpoint - no existing credit history, employment records, or financial accounts. Identity thieves exploit the gap between Social Security Administration records and credit bureau reporting. When a child gets a social security number, it's reported to SSA but not automatically sent to credit bureaus. Thieves take this "clean" social security number and create a fictitious identity by combining it with fake names, addresses, and birthdates. They then apply for small lines of credit to establish a credit profile, which enables them to obtain additional accounts. The theft often goes undetected for years because parents don't typically check their children's credit until they're ready to apply for financial aid or their first legitimate accounts.

Q2: How has AI technology changed the landscape of scams targeting young people, particularly in sextortion cases?

A: AI has dramatically escalated the sophistication and effectiveness of scams targeting youth. Deepfake technology now allows scammers to create convincing fake videos of influencers promoting "exclusive deals," making it much harder for young people to distinguish legitimate from fraudulent content. In sextortion cases, AI enables scammers to create fake profiles that are increasingly realistic, and even allows them to manipulate non-sexual photos to appear explicit, giving them leverage over victims. Traditional verification methods like video calls are no longer reliable because deepfake technology can create real-time fake video interactions. This makes it much easier for scammers to convince young people they're talking to legitimate peers or influencers, dramatically increasing the success rate of these predatory schemes.

Q3: What are the warning signs that a child's identity may have been stolen, and when do parents typically discover this theft?

A: Key warning signs include children receiving pre-approval credit card offers, notices from the IRS about tax returns filed using the child's social security number (when parents have claimed the child as a dependent), contact from debt collectors or lenders about accounts the child never opened, and denials for student loans due to poor credit history. The most common discovery point is when families begin preparing for college and apply for financial aid. Many parents are shocked to learn their child has an extensive credit history with poor payment records, sometimes spanning several years. This timing is particularly devastating because it can impact the child's ability to secure student loans or even housing for college. Some parents also discover the theft when children receive government benefits notices or utility companies contact them about unpaid bills in the child's name.

Q4: What safety measures should parents teach their children about peer-to-peer payment apps and social media shopping?

A: Parents should educate children never to share login credentials for payment apps and to be extremely suspicious of any "earn money" opportunities or prize offers that require upfront payments or transfers. For social media shopping, teach children that legitimate companies don't send individual direct messages to sell products - this should always be treated as a scam. When buying from influencers, verify the video is from the influencer's actual verified profile account (look for platform verification badges). Avoid paying through peer-to-peer apps like Cash App or Venmo for purchases, as these offer limited buyer protections compared to PayPal or credit cards. Parents should offer to review any purchase before their child completes the transaction, positioning this as a safety measure rather than control. Children should also understand what constitutes personal information (address, birthdate, school information, license numbers) and never share this in online interactions.

Q5: How should parents respond if their child becomes a victim of sextortion, and what are the recommended next steps?

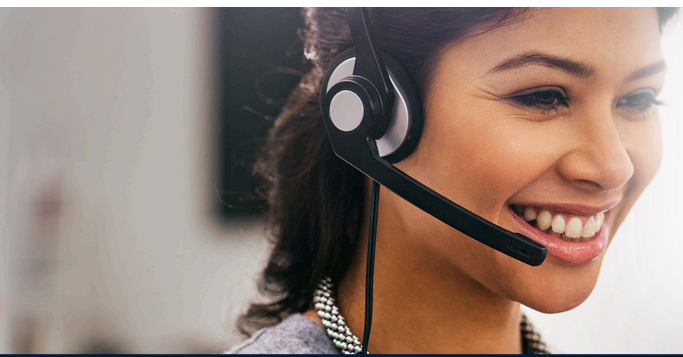
A: First, report the account to the platform immediately so they can shut down the profile and prevent the scammer from targeting other children. Block the perpetrator and save all messages and profile information as evidence. Report the incident to IC3 (Internet Crime Complaint Center) under the FBI, which collects data to help law enforcement recognize patterns and potentially catch perpetrators. Many of these crimes are committed internationally, but law enforcement focuses on catching the domestic money laundering components to disrupt the networks. If the child is on Snapchat, use their new reporting reason specifically for sextortion to help them track trends and patterns. Parents should approach this as a crime against their child, not something the child did wrong, and provide emotional support while taking these investigative steps. The goal is to cut off the scammer's access while providing law enforcement with intelligence that could help protect other children.

About Our Speaker:

SAHARA SEARS LEGAL RESOURCES

Sahara Sears is the Head of Business and Product Development at Legal Resources, a legal and identity theft plan provider based in Virginia Beach. She leads the research and content development for the company's educational seminars and frequently presents on legal and identity theft topics to employees, employers, and professional associations. She holds a Bachelor's of Applied Science in Criminal Justice and is certified as an Identity Theft Risk Management Specialist, Private Investigator, and Paralegal.

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