ndi | 20 YEARS OF IMPACT
ESTABLISHED 2005

Identity Theft and Scam Prevention: What's Changed, What Hasn't...

Presented By

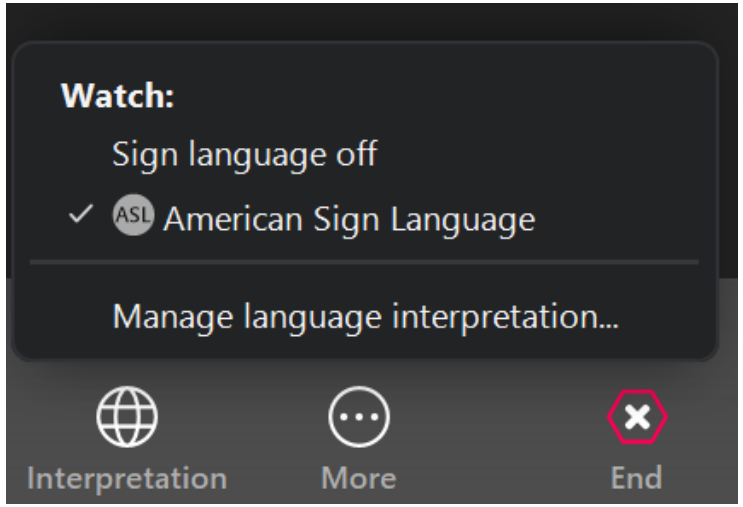
NDI's Financial Resilience Center
and Experian

Todays' event is brought to you by NDI's Financial Resilience Center

With generous support from

ASL Interpretation

- ASL interpretation has been arranged for this webinar. There will be two interpreters for this event, and they will switch off periodically.
- To view the ASL interpreter, navigate to the menu bar at the bottom of your screen and click on “Interpretation.” Select “American Sign Language” to view the interpreters in a separate video pane.



Audio and Captions

- The audio for today's meeting can be accessed using Computer Audio or by calling in by phone. If you select Computer Audio, please make sure your speakers are turned on or your headphones are plugged in.
- To call in for audio:
  - Dial: 877-853-5257
  - The meeting code is 881-7954-5189
- Real-time human captioning is being provided. The captions can be found by clicking on the "cc" button in the Zoom controls at the bottom of the screen.
- If you do not see the captions after clicking the "cc" button, please alert the host via the Q&A box.

Questions and Technical Assistance

- Please send your questions, concerns and any requests for technical assistance to the NDI Host via the Q&A box.
- Questions will be addressed by the presenter if time allows.
- If your question is not answered during the webinar, you are listening by phone or you are unable to use the Q&A box, please email Liz Layman at elayman@ndi-inc.org.
- Please note: This webinar is being recorded, and the materials will be available on the FRC page within 1-2 weeks.

National Disability Institute (NDI)

NDI is a national nonprofit organization dedicated to building a better financial future for people with disabilities and their families. The first organization committed exclusively to championing economic empowerment, financial education, asset development and financial stability for all persons with disabilities for the past 20 years.

What we do:

- Build capacity of the field through training and technical assistance
- Drive systems change by implementing models that can be replicated
- Test innovative approaches to financial empowerment
- Lead research to uncover barriers and opportunities
- Advance change through public education and policy development

NDI's Financial Resilience Center (FRC)

FinancialResilienceCenter.org

Financial resilience, the ability to bounce back through difficult times, emerge stronger on the other side and flourish in the "new normal."

FRC Overview

- Timely, up-to-date and accurate information, alerts, financial tools and resources
- Analysis of federal policy and impact
- Resources provided in easy Q&A format under topic areas of interest
- Email sign-up to receive our newsletter, updates and alerts, including upcoming and past recordings of webinars

Today's Presenters

Mike Bruemmer
Head of Global Data Breach Resolution
Experian

Becky MacDicken
Director, Financial Empowerment
National Disability Institute

Agenda

- Avoiding Identity Theft | Financial Resources for People with Disabilities
- What hasn't changed?
- What's new?
- Resources
- Q&A

Identity Theft and Scam Prevention

experian™

Identity Theft vs. Scams

Identity Theft - Identity theft occurs when someone steals your personal information—like your Social Security number, bank account details, or driver's license—and uses it to impersonate you or commit fraud.

Examples:

- Opening a credit card in your name
- Filing a fake tax return to claim your refund
- Creating a fake ID using your personal details

Scams - Scams are deceptive schemes designed to trick you into giving away money or personal information. They often involve manipulation, lies, or impersonation.

Examples:

- Phishing emails pretending to be your bank
- Romance scams where someone builds a fake relationship to ask for money
- Tech support scams claiming your computer is infected

What hasn’t changed?

- Scammers are still around and getting more organized
- AI is the newest frontier-faster, better, cheaper
- Disabled consumers are in the Top 3 targets

    1-Young adults

    2-Sr Citizens

    3-Disabled people

The Latest Data

General Identity Theft Trends

• The FTC received 5.7 million fraud reports in 2025, including 1.4 million identity theft cases.

• The most common type of identity theft was Government Documents or Benefits Fraud, with nearly 396,000 cases—a category that disproportionately affects people with disabilities who rely on public benefits.

Protecting the Disabled Community from Fraud

- Identity theft occurs due to an overreliance on caregivers or other parties to manage finances leaves disabled individuals vulnerable. Personal identifying information (PII) is stolen and used to apply for credit, files taxes, and procure medical services.
- Financial scams involve tricking disabled individuals to give away their money or personal information due to their trust and goodwill.
- Financial scams include lottery scams, romance scams, investment scams.
- Employment scams

What's New?

- Govt Impersonation for stealing benefits, especially medical
- $$$ earned working from Home
- Job Postings and Interviews
- Medical/healthcare services and discounts
- Medicaid and Medicare fraud

Examples

- VA Disability Benefits (Puerto Rico)-Insider stealing lifetime benefits
- 3rd party Trust Benefit Administrator-$100M taken by Founder and CFO
- Nursing home staff tipping off scammers where people are incapacitated
- Ring of caregivers in State Hospital that stole PII from patients
- People impersonating a loved one who is in trouble who needs money

Cryptocurrency: Key warnings and recent developments to be aware of:

Common Cryptocurrency Scams

- Impersonation Scams: Fraudsters pose as government officials, banks, or celebrities to trick you into sending crypto.
- Investment Scams: Promises of high returns lure victims into fake platforms or "pig butchering" schemes, where scammers build trust before disappearing with your money.
- Romance Scams: Scammers build emotional relationships online and eventually ask for crypto payments, often via Bitcoin ATMs.
- Blackmail & Extortion: Threats to release compromising information unless paid in cryptocurrency.

Bitcoin ATM Risks

- Bitcoin ATMs are increasingly used in scams. Victims are told to deposit cash and send crypto to a scammer's wallet via QR code.
- The FBI reports losses of nearly $250 million from Bitcoin ATM scams in 2024 alone.

Safety Tips

- Never send cryptocurrency to settle debts, pay taxes, or resolve legal issues—real authorities don't ask for crypto.
- Be skeptical of unsolicited investment offers or emotional appeals online.
- Double-check sources before making payments, especially if pressured.

You can find more guidance from the FTC:
What To Know About Cryptocurrency and Scams | Consumer Advice

Artificial Intelligence (AI) – How it's used to Scam

- Voice Cloning in Grandparent Scams: Scammers use AI to mimic a loved one's voice, calling older adults with urgent pleas for help. These scams have defrauded victims of over $21 million across 40 states.
- Deepfake Impersonations: Fraudsters create realistic videos or audio clips of executives, celebrities, or officials to trick people into sending money or sensitive data.
- AI-Generated Phishing Emails: These emails are grammatically perfect and personalized, making them harder to spot. They often impersonate banks or government agencies.
- Synthetic Identity Fraud: AI tools generate fake identities that pass verification checks, allowing scammers to open accounts or apply for loans.
- Fake Job Offers & Shopping Sites: AI helps scammers create convincing websites and job postings. Victims may receive fake checks or be asked to send money upfront.

How to Protect Against AI

- Verify urgent requests through known contacts—don't trust caller ID.
- Use two-factor authentication on all accounts.
- Be skeptical of unsolicited messages, especially those asking for secrecy or immediate action.
- Educate family members, especially older adults, about voice cloning and deepfake risks.
- Report suspicious activity to local law enforcement or the FBI's Internet Crime Complaint Center.
  Home Page - Internet Crime Complaint Center (IC3)

Which threats are current?

- Anything powered or supercharged with AI - audio, video, biometric
- Text scams - unpaid taxes, tolls, medical or pharmacy benefits.
- Deepfake phone calls
- Good old email and snail mail

Red Flags

Remember SURF

- Scare/fear
- Urgency
- Random
- F(ph)ishing

Prevention Musts

- Freeze your credit file at all the bureaus
- Use a password manager (Keeper)
- Shred docs every month
- Free spam block from your cell phone provider
- Ditch the land line
- Always verify and never trust
- Third party (non-family) vetting of offers, calls, communication
- Two factor authentication
- Report scam attempts to ReportFraud@ftc.gov

What to do if you become a victim

- Freeze your credit
- Check your free credit reports annually
- Close accounts that have been tampered with
- Change passwords on important accounts
- File a police report
- Report to the Federal Trade Commission
- Take advantage of FREE IndentityWorks protection

Tools and Resources

- Data Breach FAQs for Consumers
- Experian ID Works Common Questions
- Fraud Resolution by Experian FAQ
- How to Freeze Your Credit at All 3 Credit Bureaus
- IdentityTheft.gov
- Identity Theft Resource Center | ITRC
- Financial Resources for People with Disabilities (Financial Resilience Center)
- Crédito | Financial Resilience Resources for People with Disabilities

Questions?

Thank you!