

IDENTITY THEFT TODAY

Outsmarting Authorized Push Payment Fraud

September 16, 2026
12pm - 1pm EST



SESSION NOTES

Below is a summary of the topics and items discussed on the September 16, 2026 session of **Identity Theft Today: Outsmarting Authorized Push Payment Fraud** featuring guest speakers Bill Sallurday.

These notes were compiled following a virtual webinar presentation and are provided for general informational purposes only. The session was presented by an attorney licensed in a specific state. Attorneys are not licensed in every state, and laws, regulations, terminology, and requirements vary by jurisdiction. This content is not legal advice and should not be relied upon as such. While best efforts were made to accurately capture the discussion, this document is a transcription summary and may contain errors, omissions, or inaccuracies in wording, facts, or interpretation. Legal Resources and the presenter are not responsible or liable for any consequences that may arise from reading, using, or interpreting this material. For legal advice specific to your situation, please consult with a qualified attorney licensed in your state.

SESSION TOPICS

APP fraud | Imposter Scams | Romance Scams | Investment Scams
AI/Deepfakes | Invoice Fraud | Credit Freezes | Scam Recovery

[Click Here to Access Recorded Session](#) →

LIABILITY HAS SHIFTED

- Regulation E protects consumers on unauthorized transactions — the bank must reimburse
- APP fraud is different: if the scammer tricks you into sending the money yourself, the bank isn't required to return it
- 2019: the largest Zelle banks reimbursed roughly 62% of these losses. By 2023 that dropped to 38%
- Practical takeaway: the burden has moved to the consumer, which makes prevention the only reliable protection

SCALE OF LOSSES

- FTC reported \$16 billion lost in 2025 — the highest on record, and considered a floor since it only reflects what was reported
- Imposter scams alone: \$3.5 billion, nearly triple 2020 levels
- Romance scam victims over 60 lost close to \$600 million in 2025
- Losses are outpacing case volume: scammers are extracting more money per victim
- Peer-to-peer apps (Zelle, Venmo, PayPal) and business email compromise are both growing fast

ANATOMY OF SCAMS

Four-step playbook:

1. **Uninitiated contact** — an email, text, call, or letter you didn't request
2. **A compelling reason to act** — built on fear (grandparent scams), greed that's often really need (bills stacking up), or isolation (romance scams)
3. **A request for nontraditional payment** — wire, P2P app, gift cards, crypto ATM
4. **Urgency at every step** — even in long-game scams, each individual ask is rushed

Recognition tip: uninitiated contact is the earliest tell. Hang up, go "out of band," and call back on a number you looked up yourself.

SCAM TYPES COVERED

- **Impersonation** — including a celebrity/athlete fan page case that escalated into an investment scam
- **Romance** — now including AI-generated video calls, which used to be a reliable screening test
- **Investment / "pig butchering"** — legitimate-looking app from the App Store, fake gains, then endless fees to withdraw before the site goes dark
- **Purchase scams** — tickets and marketplace goods that never arrive
- **Invoice fraud and BEC** — fake supplier invoices paid through legitimate channels
- **Social engineering** — public records plus social media give scammers a complete profile

AI RAISES STAKES

- Deepfake video and voice cloning are accelerating grandparent scams
- AI enables scams at scale: bots run the early stages, then hand off to a human closer
- Supervised AI – useful as a tool, but validate what comes out of it

RED FLAGS DISCUSSED

- Secrecy and urgency ("don't tell your family, you'll jeopardize the investigation")
- Unusual payment requests — no legitimate organization takes gift cards
- "Your account is compromised, move your money to a safe account" — banks never ask this
- Being told your own account number or SSN is **not** proof of legitimacy. Over 6.7 billion records had been breached by 2017 and scammers assemble profiles piece by piece

PREVENTION STEPS RECOMMENDED

- **Pause before you pay** — no legitimate request is too urgent to verify by phone first
- Call the real number (back of the card), never a link in the message
- Set a family safe word in advance
- Credit freeze with all three bureaus (Experian, TransUnion, Equifax) — his number-one recommendation regardless of age
- Turn on transaction and transfer alerts at your financial institution
- Deed/title alerts through your county assessor's office

IF IT HAPPENS

- Act immediately — call the bank and report it as unauthorized
- File with the FTC and the FBI's IC3.gov; contact local law enforcement and your state attorney general
- Document everything in writing from the moment you suspect a problem
- Don't let shame keep you quiet — timing and circumstance, not intelligence, determine who falls for these

Q&A HIGHLIGHTS

Q1: Why do gift card scams work so well?

Gift cards are both easy to find and share. Scammers coach victims on exactly what to say if a cashier asks questions. Retailers and the FBI have improved interdiction — an Arizona cashier recently stopped an elderly customer mid-purchase — but gift cards remain a red flag. Any request to pay with them should trigger a pause.

Coming Up Next Month

**AI and Data Privacy:
Protecting Yourself in a
Rapidly Changing World**

October 14, 2026
12pm - 1pm EST

Register at www.LRseminars.com

Q&A HIGHLIGHTS

Q2: If I click a link and the scammer gains access to my account, is that still "authorized"?

That's where the legal nuance sits, and it's worth reviewing with an attorney. It usually starts the same way: an uninitiated pop-up claiming your computer is infected, with a number to call. Pause before granting access, and contact the company directly.

Q3: Do I have to freeze my credit with each bureau separately, and how do I unfreeze it?

Yes — freeze with all three individually. A freeze locks your credit file against new account openings; it does not affect your existing cards. When you need credit, ask the lender which bureau they pull and thaw just that one, for a day or a week, through the bureau's app.

Q4: Is there protection against title and deed fraud? Do home title lock services work?

The speaker declined to endorse specific monitoring products. His recommendation: register for deed alerts with your county assessor so you're notified of any filing against your property. Property owned free and clear, and vacant land, are the highest-risk categories. Some owners place a zero-balance home equity lien as an added hurdle — a question for your financial and tax advisors.

Q5: Someone opened a credit card in my name and I didn't know for months. What now?

Go back to the issuing institution and dispute it — they carry responsibility for verifying identity at account opening, and the account was likely opened at a different address. A credit freeze is the best prevention. This is also a good point to involve your Legal Resources attorney.

ABOUT THE SPEAKER:



BILL SALLURDAY | R.O.S.E.

Bill Sallurday serves on the board of R.O.S.E. (Resources/Outreach to Safeguard the Elderly), an Arizona nonprofit whose mission is to prevent the financial exploitation and defrauding of older adults. At R.O.S.E. he leads scam-prevention education for consumers and their families, drawing on five years of tracking authorized push payment fraud trends, and works with legislators on consumer protection measures in Arizona.

DISCLAIMER: This summary highlights key webinar points and questions. For comprehensive details, view the full seminar at [LRSeminars.com](https://www.LRSeminars.com).

Contact Us

Our Member Services team is available for assistance.

Phone: 800.728.5768

Email: info@legalresources.com

www.legalresources.com