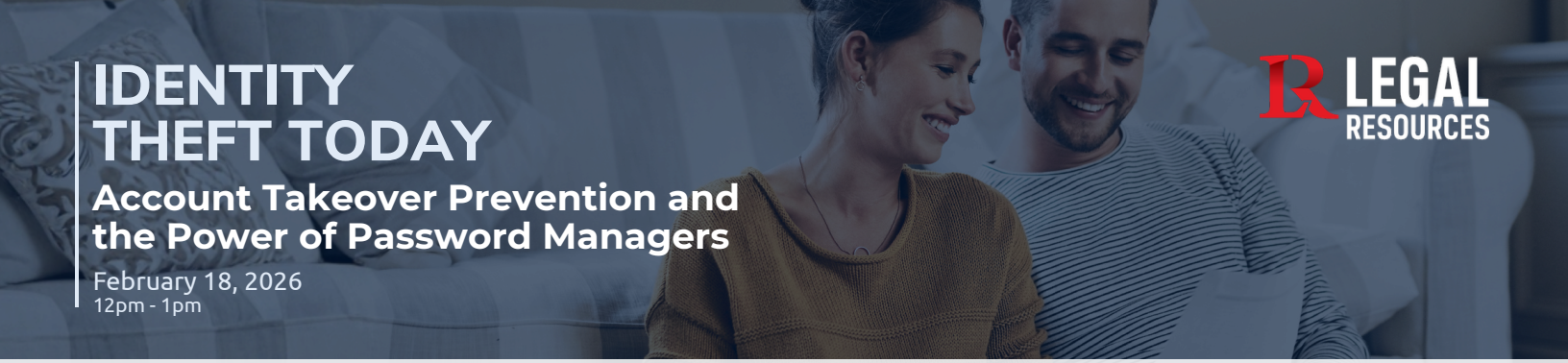


# IDENTITY THEFT TODAY

## Account Takeover Prevention and the Power of Password Managers

February 18, 2026
12pm - 1pm

LEGAL RESOURCES

### SESSION NOTES

Below is a summary of the topics and items discussed on the 2/18/2026 session of the **Identity Theft Today Seminar: Account Takeover Prevention and the Power of Password Managers.**



### SESSION TOPICS

Account Takeover Basics | Credential Theft Methods | Compromise Warning Signs
Password Manager Benefits | Multi-Factor Authentication| Victim Recovery Steps

**Click Here to Access Recorded Session** ⟶

## ACCOUNT TAKEOVER BASICS

- Account takeover occurs when an unauthorized person logs into your account using stolen credentials — any online account is at risk, including email, banking, social media, healthcare, and payroll
- Once inside, criminals can transfer money, steal personal data, find stored payment methods, and use the account to launch further attacks
- Nearly 29% of U.S. adults experienced account takeover in 2024; fraud losses reached nearly $13 billion in 2023, with attack volume growing 141% over four years

## CREDENTIAL THEFT METHODS

- **Data Breaches**: 3,158 publicly reported breaches occurred in 2024; over 1.7 billion breach notifications were sent to consumers that year
- **Credential Stuffing**: Automated software sprays breached username/password combinations across hundreds of websites — 26 billion attempts per month mean even a tiny success rate yields millions of compromised accounts
- **Phishing & Social Engineering**: Criminals impersonate trusted brands via email, text, or phone to harvest credentials, using urgency and fear to prevent victims from stopping to verify
- **SIM Swapping, Malware & SEO Poisoning**: Additional methods used to steal credentials or redirect users to fake login pages

## COMPROMISE WARNING SIGNS

- Password reset or account change emails you did not initiate
- Login alerts from unfamiliar devices or locations
- Unexpected two-factor authentication codes — this may mean someone already has your password and is attempting entry
- Missing funds or unfamiliar transactions on financial accounts

## PASSWORD MANAGER BENEFITS

- The average user has ~150 online accounts; 81% admit to reusing passwords — reuse is a primary driver of account takeover
- Passwords must be at least 16 characters, random, and unique per site — an 8-character password can be brute-forced in 30 minutes; a 16-character password would take roughly one million years
- Password managers generate, store, and auto-fill strong passwords across all devices; your only responsibility is one strong master password
- Reputable options include Bitwarden, Keeper, LastPass, and 1Password; many free versions cover all core features

**Coming Up Next Month**

**App Tampering and Code Injection: The Hidden Threat Inside Your Apps**

March 18, 2026
12pm - 1pm

*Register at www.LRseminars.com*

## MULTI-FACTOR AUTHENTICATION

- MFA combines something you know (password), have (phone/key), and are (fingerprint/face ID), making a stolen password alone insufficient
- Authenticator apps are more secure than SMS codes; passkeys are an even stronger emerging alternative that skip passwords entirely
- Never share a two-factor code with anyone who contacts you — legitimate companies will never ask for it

## VICTIM RECOVERY STEPS

- Contact your financial institution immediately if money has moved without authorization
- Change passwords, enable MFA, and file a complaint at **IC3.gov**
- Check your exposure at **haveibeenpwned.com** and freeze your credit at **frozenpii.com**
- Contact the **Identity Theft Resource Center** (toll-free) for personalized recovery support

## KEY TAKEAWAYS

1. Use a password manager — it is the most practical way to maintain unique, strong passwords at scale
2. Enable multi-factor authentication everywhere, especially on email and banking accounts
3. Never reuse passwords — one breached site puts all accounts sharing that password at risk
4. Be skeptical of all inbound, urgent messages — hang up and call back using a number you independently verified
5. Monitor accounts regularly and act quickly if unauthorized activity appears

## Q&A HIGHLIGHTS

**Q1. A company used my information to submit a false health insurance claim. I've alerted my insurer — what else should I do?**
**Answer:** Disputing the fraudulent claim promptly is the primary action available. Unfortunately, with the volume of data already exposed through past breaches, that information is difficult to fully contain. Staying alert and disputing claims as they surface is the best ongoing approach.

**Q2. Are passkeys better than passwords?**
**Answer:** Yes. Passkeys skip the password entirely and rely on device-based biometrics — something you have and something you are — making them far harder to steal through phishing. The current limitation is that most services still allow password login as a fallback, so strong passwords and MFA remain important in the meantime.

**Q3. Do free password managers work across multiple devices?**
**Answer:** Yes — most sync automatically across all devices once the app or browser extension is installed and you're logged in with your master password. This cross-device functionality is essential, since manually transferring long, randomly generated passwords between devices would be impractical.

**Q4. If I pass away, how can my family access my password manager?**
**Answer:** Many password managers offer a family sharing or trusted contact option for emergency access. A shared family vault or joint account with a partner is another strong option. Writing down your master password and storing it securely is a reasonable backup. Including account access instructions in a "digital will" as part of your broader estate planning is also worth considering.

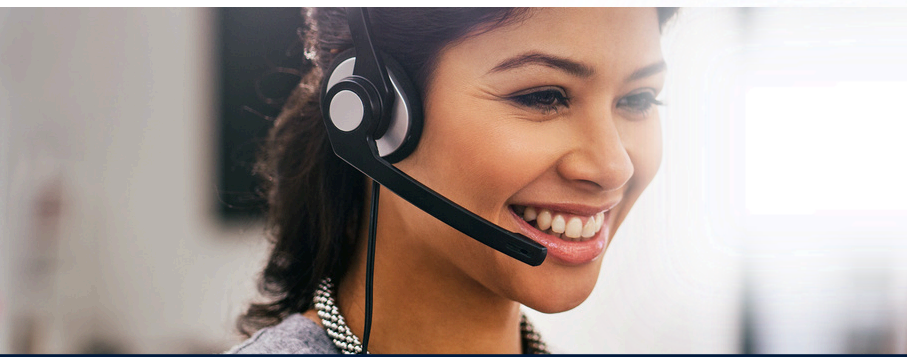
**Q5. Are there fake password managers, and how do I know if one is legitimate?**
**Answer:** Fake password managers do exist. Download only from official app stores, verify the developer name matches the company, and look for a high volume of reviews. Visiting the password manager's official website directly and following their download link is the safest approach. Review sites like PCMag, Wired, and Consumer Reports can also help confirm legitimacy.

## ABOUT OUR SPEAKER:

### CLIFF STEINHAUER | NATIONAL CYBERSECURITY ALLIANCE

Cliff Steinhauer is a cybersecurity expert and Director of Information Security and Engagement at the National Cybersecurity Alliance (NCA), where he has worked for over four years. He leads NCA's internal security program and conducts educational outreach through webinars and presentations nationwide. Additional resources are available at **staysafeonline.org**.

**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