# IDENTITY THEFT TODAY

## So You've Been Breached

January 15, 2025
12pm - 1pm

LEGAL RESOURCES

## SESSION NOTES

Below is a summary of the topics and items discussed on the January 15, 2025 session of **Identity Theft Today, So You've Been Breached**.

***A recording of this session is available for viewing at www.LRseminars.com***



## SESSION TOPICS

- Data Breach Statistics
- Impacts of Exposure
- Securing Exposed Data
- ID Theft Resources
- Fraud Alerts & Credit Freezes
- Credit Report Dispute & Resolution

### Incidents vs. Breach

All breaches are incidents, but not all incidents are breaches. Incidents compromise the integrity, confidentiality, or availability of information or systems but do not necessarily result in data loss or unauthorized access. Breaches are confirmed incidents where data or sensitive information has been accessed, stolen, or exposed to unauthorized parties.

### Key Statistics

- Over 30,000 reported security incidents were analyzed in 2023 and over 10,000 were confirmed as data breaches.
- Ransomware accounted for over 20% of all breaches and affected 92% of industries.
- Human element remained a top vulnerability at almost 70%.
- Exploitation of vulnerability attacks increased by 180% over the last year.

### What happens to all the data from a breach?

Compromised credentials are often monetized and sold on dark web marketplaces, forums, and websites.

### What are the potential impacts of being involved in a data breach?

- **Financial Harm:** Scammers could use your personal information to open loans or credit cards in your name, leaving you responsible for debts you didn't incur.
- **Identity Theft:** Your Social Security number or other identifying details could be used to impersonate you, potentially causing legal, financial, or reputational damage.
- **Loss of Privacy:** Sensitive details, like your medical records or private communications, could be exposed, leaving you feeling vulnerable and violated.
- **Emotional Stress:** Knowing that your personal data is in the hands of criminals can create anxiety and fear about what they might do with it.
- **Targeted Scams:** Compromised credentials are often monetized and sold on dark web marketplaces, forums, and websites.
- **Long-Term Vigilance:** You might need to monitor your credit reports and accounts for years to safeguard against potential misuse of your stolen data.

## What steps should you take after a breach?

1. Assess the Type of Data Impacted
   a. Review breach notification details (carefully review the notification to identify specific categories of compromised data, such as personal, financial, sensitive information, and login credentials).
   b. Understand what specific information was compromised.
   c. Contact the organization that exposed your information or notified you for additional details if needed.


2. Secure Compromised Data
   Secure impacted data as quickly as possible

| Type of Data Exposed | Actions to Secure Data |
|---|---|
| Username and Password | • Change passwords immediately for exposed accounts.<br>• Use strong, unique passwords.<br>• Avoid reusing passwords across multiple accounts. |
| Credit Card Information | • Contact your bank or credit card company.<br>• Freeze the affected account.<br>• Request a new card to prevent unauthorized transactions. |
| Health Insurance Member Number | • Contact your health insurance provider.<br>• Request a new member ID to prevent fraudulent use of benefits. |
| Social Security Number | • Place a fraud alert or credit freeze on your credit reports.<br>• Monitor credit activity and watch for suspicious activity. |

3. Place an Alert and/or Freeze
   a. Place a fraud alert or credit freeze.
      i. Fraud Alert: Place with one credit bureau, and it applies to all three
         1. Initial (1 year).
         2. Extended (7 year): Must provide supporting docs such as FTC form or Police Report; doesn't have to be evidence of damage, just evidence of identity theft.
         3. Active Duty (1 year): Provides an extra verifications step for lenders (for Military).
      ii. Credit Freeze: must request individually for each bureau.
         1. Blocks access to your credit report for new accounts by masking your credit profile from lenders.
         2. Requires lifting for new credit applications.
4. Monitor Your Information
   a. Request your credit reports once a year through annualcreditreport.com (Review inconsistencies, discrepancies and personal information).
   b. Thoroughly review your explanation of benefits statements from health insurance providers to ensure you are not being billed for medical services you did not receive.
   c. Watch for suspicious activity such as unfamiliar accounts, unauthorized inquiries and other signs of fraud.
   d. Monitor existing account balances, credit limits and open/closed statuses.

## Q&A Highlights

**Q: What should I do if my bank account shows attempted unauthorized access?**

**A:** Enable multi-factor authentication, contact the bank to learn about additional security features, monitor account activity regularly, and consider setting up account alerts.

**Q: How secure are password managers?**

**A:** They are more secure than strong passwords in spreadsheets as they use encryption and security standards. They also require a master password and usually multi-factor authentication. It is important to research different password managers and their security history.

**Q: What should I do if someone opens accounts in my name?**

**A:** Contact the institution directly through official channels, file a police report, if required, check credit reports for unauthorized accounts, consider a credit freeze, and document all communications.

## TIPS TO PREVENT IDENTITY THEFT AND SCAMS

1. Utilize a password manager and use different passwords across all online accounts.
2. If you're notified that you were included in a breach, take action immediately.
3. Be cautious of unsolicited calls about accounts, do not share any information with someone who's contacted you via an inbound call.
4. Check credit your reports regularly.
5. Consider freezing your credit profiles as a preventive measure.
6. Subscribe to the FTC's scam alert newsletter.
7. Enable multi-factor authentication on your accounts when available.
8. Regularly monitor your existing online and financial accounts for suspicious activity.

## RESOURCES

- **Federal Trade Commission (FTC): identitytheft.gov**
- **Consumer Financial Protection Bureau (CFPB)**
- **Identity Theft Resource Center (free victim assistance)**
- **Annual Credit Report: annualcreditreport.com**
- **Credit Bureaus: Equifax, Experian, TransUnion**

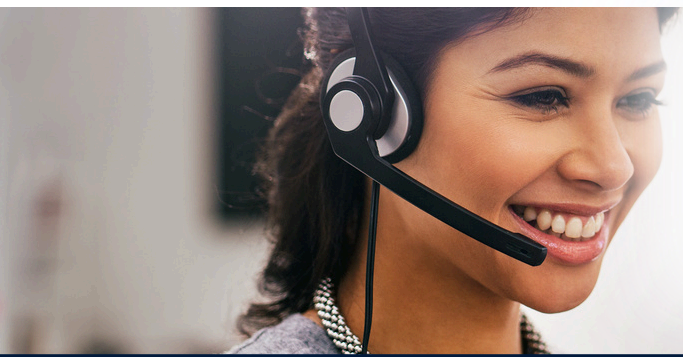
## ABOUT OUR SPEAKER:

**SAHARA SEARS**
**LEGAL RESOURCES**

Head of Business and Product Development at Legal Resources, a Legal and Identity Theft plan provider headquartered in Virginia Beach. Leads the research and content development for Legal Resources' Legal and Identity Theft educational seminars and regularly presents for employees, employers, and professional associations on these topics each year. Additionally, Sahara currently serves as a Board Member for the Peninsula Chapter for the Society of Human Resources Management (PenSHRM).

**Education:**
Bachelor's of Applied Science in Criminal Justice, University of South Florida

**Certifications:**
- Identity Theft Risk Management Specialist
- Private Investigator
- Paralegal



## Contact Us

Our Member Services team is available for assistance.

Phone: 800.728.5768
Email: info@legalresources.com

www.legalresources.com