troutman pepper locke

On the Hook:
Understanding Personal Exposure for Data Guardians

Reviewing Sources of Personal Liability and Mitigation Strategies

Privacy + Security Forum
May 8, 2025

Introduction

Speakers:

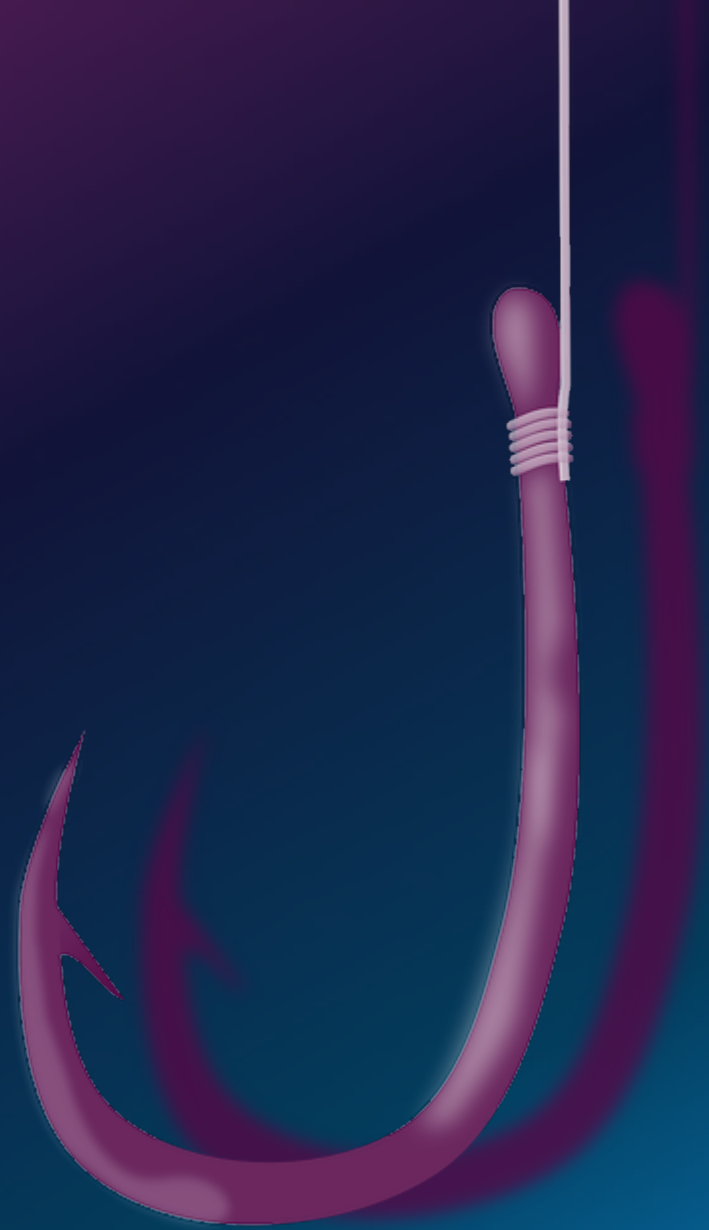
Ted Augustinos, Troutman Pepper Locke

Ryan Burch, LPL Financial

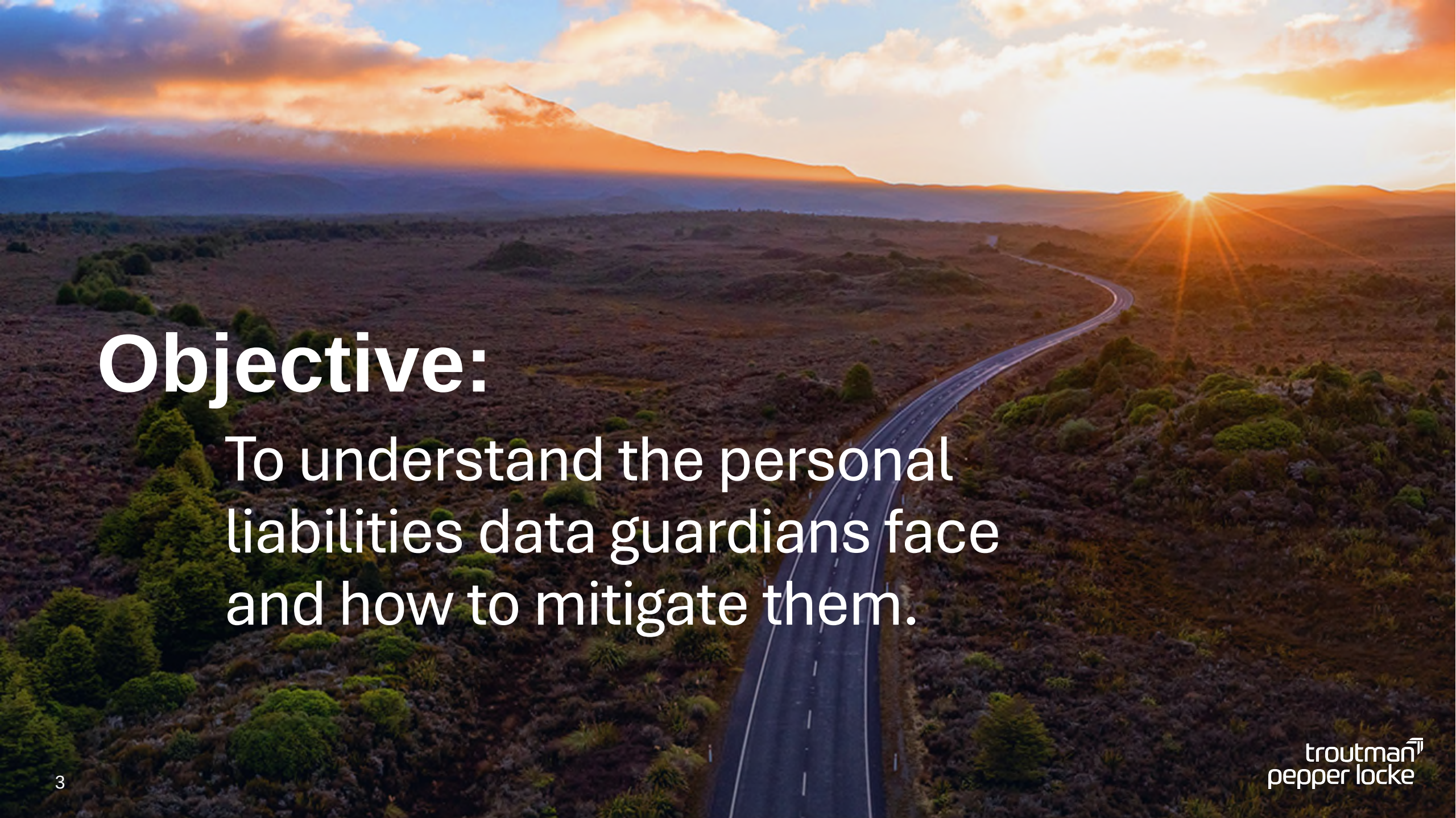
Chris Keegan, Brown & Brown

Lauren Roth, Marsh USA

Jim Shreve, Troutman Pepper Locke



troutman pepper locke



Objective:

To understand the personal liabilities data guardians face and how to mitigate them.

troutman pepper locke

Agenda

01 **Existing sources of personal liability (with case studies)**

02 **Possible additional sources of personal liability**

03 **Mitigation strategies**

04 **Q&A**

troutman pepper locke

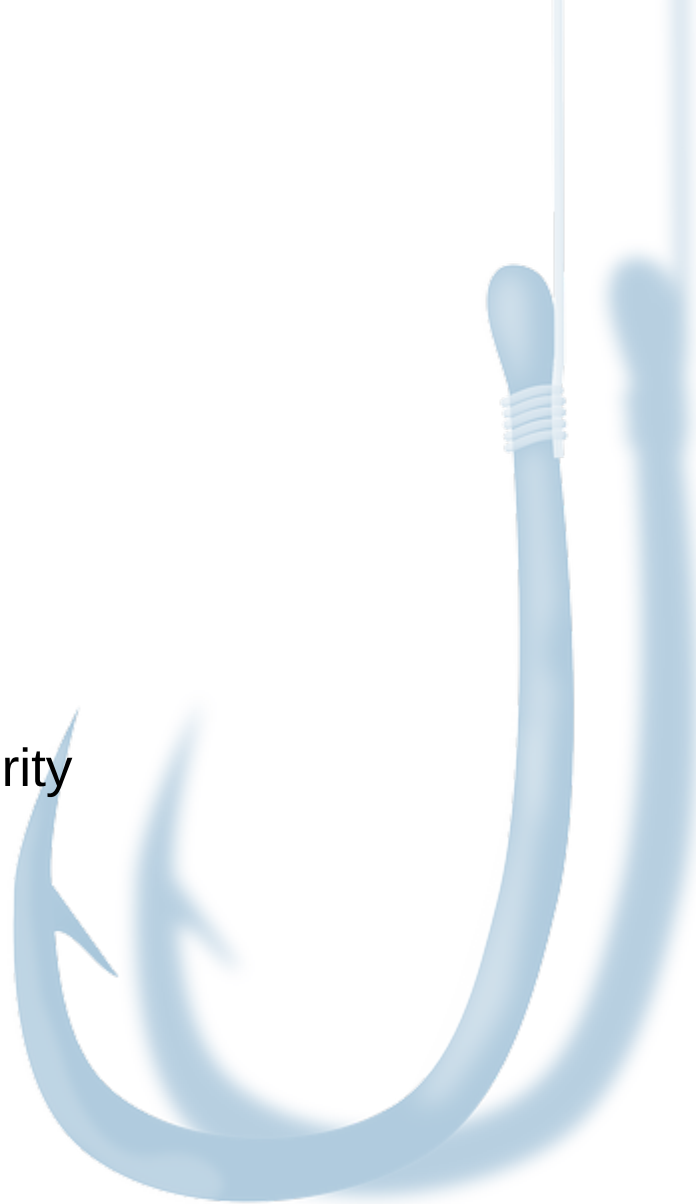
Who are the Data Guardians?

- **CISOs (obviously!)**
- **CIOs**
- **Privacy Officers**
- **Data Officers**
- **Senior Management**
- **Directors**
- **Service Providers**

troutman pepper locke

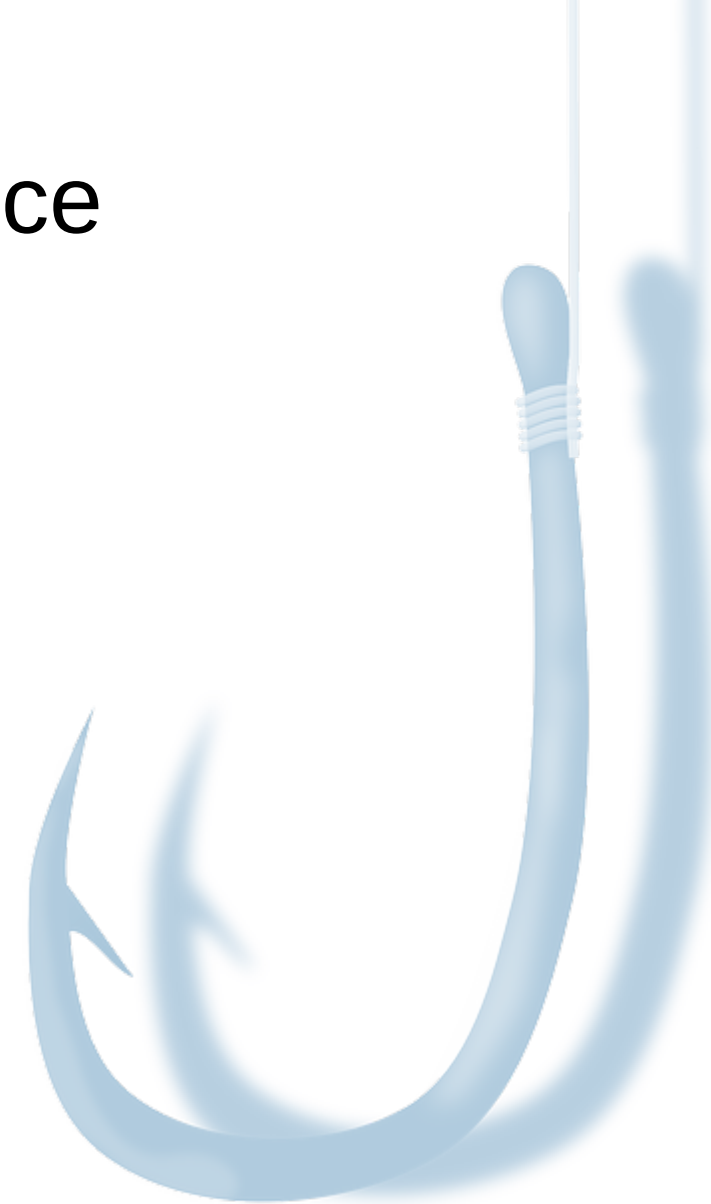
Some Legal Frameworks

- FTC Section 5
- State Breach Notification Laws and requirements for “reasonable security”
- Gramm-Leach-Bliley Act (GLBA)
- California Consumer Privacy Act (CCPA)
- New York Department of Financial Services (NY DFS) cybersecurity regulation
- Health Insurance Portability and Accountability Act (HIPAA)
- General Data Protection Regulation (GDPR)
- Shareholder derivative suits



Possible Types of Applicable Insurance

- **Cybersecurity**
- **Directors and Officers**
- **Representations and Warranties**
- **Crime**

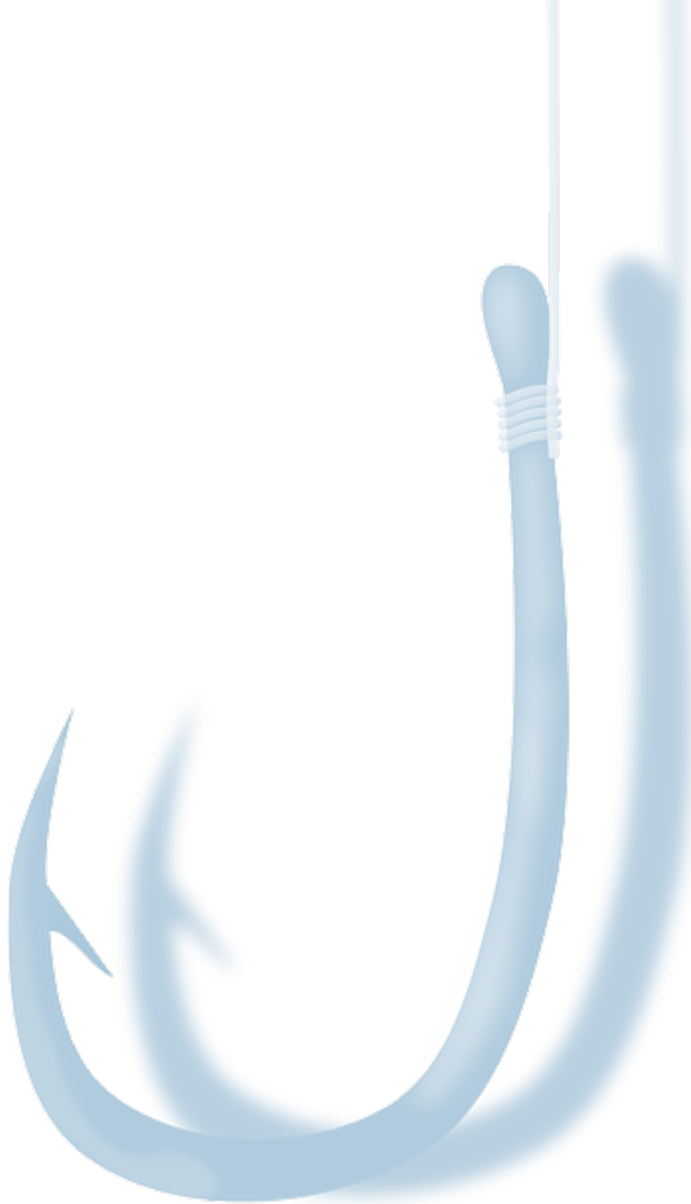


Insurance Issues to Consider

- **Assessing Insured Status**
  - Is the CISO named specifically as an Insured Person, or considered an “officer” or “employee” within the meaning of the policy?

- **Identifying Key Insuring Agreements**
  - What coverage may be triggered and whether the definitions of claim or regulatory action (or similar definitions) are satisfied.

- **Understanding scope of coverage provided**
  - Event costs, defense costs, fines, penalties, and other damages
  - Take note of any limitations and exclusions

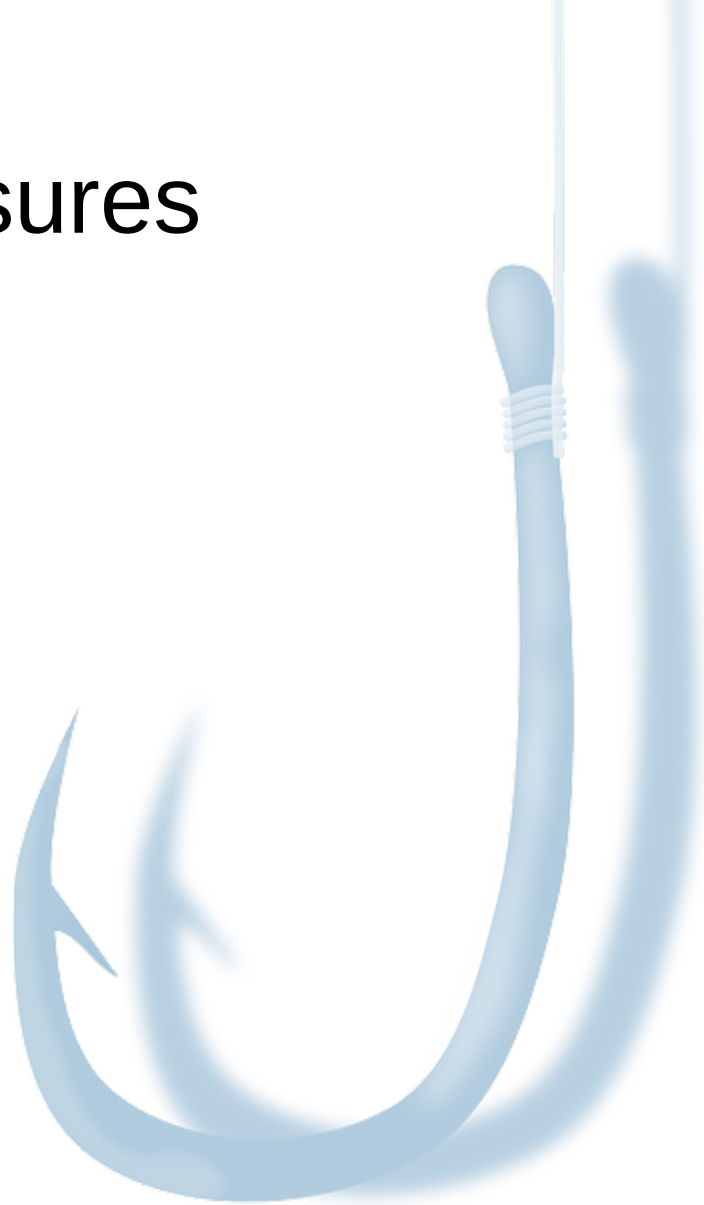


Known Causes of Potential Liability

- **Data Breaches**
- **Statements or Assertions Relating to Mergers or Acquisitions**
- **Certifications**

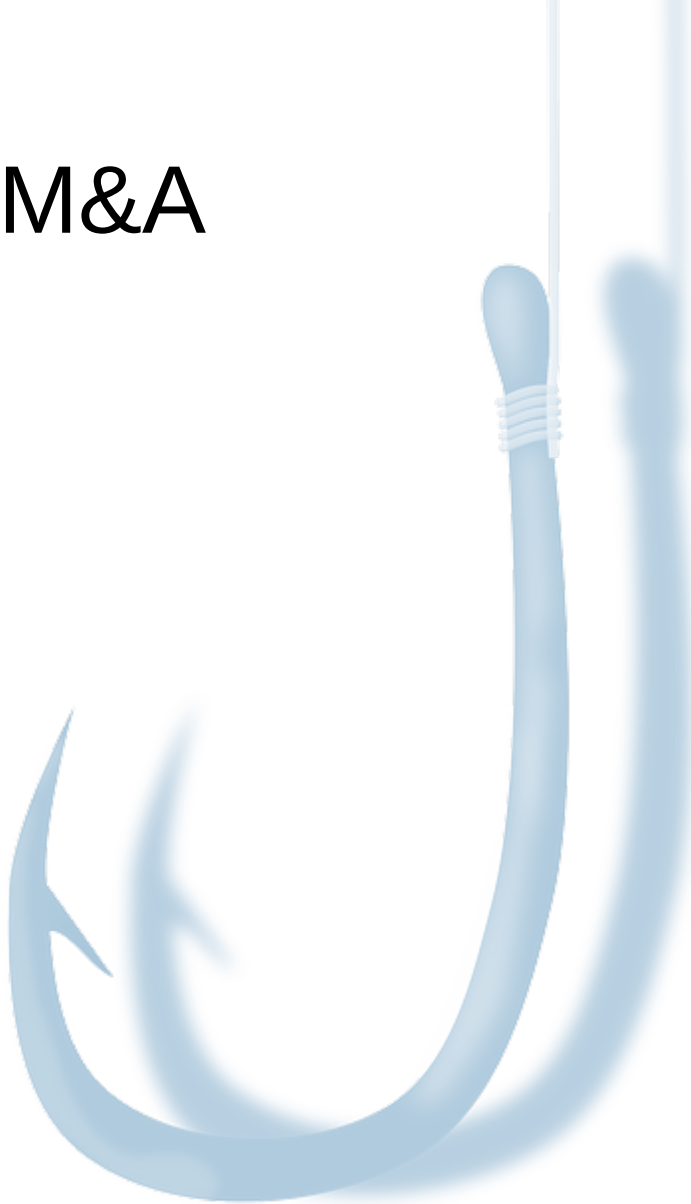
Security Breaches and Public Disclosures

- **Shareholder Derivative Suits**
- **Actions by Regulators or Law Enforcement**
- **Allegations of Breach of Fiduciary Duty**
- **What about Suits by Impacted Individuals?**



Statements or Assertions Relating to M&A

- **Shareholder Derivative Suits**



Case Study
Shareholder Derivative Suit

- **Scenario:** Company A has just closed on the acquisition of Company B. Information security at B just learned they had been the victim of an extensive hacking attack two years prior. Diligence had shown that security controls at B were below industry standards, but the breach was unknown. The board at B received perfunctory five minute semiannual updates from the CISO. The incident is being reported in the press and A's share price is down 10% since news broke.
- **Consequences:** Legal actions against board members, the CEO and CFO at A and former board members and CISO at B, financial penalties, and reputational damage.
- **Possible Insurance Treatment**
- **Lessons Learned:** Importance of good diligence and having the board and senior management connect meaningfully with the CISO.

Case Study
Regulatory or Law Enforcement Action

- **Scenario:** Company C experiences a ransomware incident involving extensive exfiltration of personal information and company IP. The company pays a ransom for return of the data, but denies any malicious intrusion and characterizes the payment as part of a bug bounty program in public statements and a 10-K filing.
- **Consequences:** Legal actions against the CEO, CFO and CISO, financial penalties from the SEC and FTC, and reputational damage.
- **Possible Insurance Treatment**
- **Lessons Learned:** Importance of accurate disclosures.

Certifications

Government Contracts

- **False Claims Act/DOJ Cyber Fraud Initiative**
- **Elements**
  - Fraud vs. non-fraud
- **Examples**
  - Centene/Health Net Federal Services
  - Penn State
  - Georgia Tech

New York DFS Certification of Compliance

- **CISO**
- **Board**

Case Study
NY DFS Certification and False Claims Act

- **Scenario:** A mortgage servicer licensed by NY DFS has filed timely certifications of compliance with the cybersecurity regulation for the last three years. Last fall the lender experienced a breach and notified DFS of the incident. The investigation revealed that the incident occurred in part from a failure to fully implement MFA and to conduct timely vulnerability scans. The servicer also services VA loans as a government contract and must comply with NIST 800-171.
- **Consequences:** Fines for non-compliance with DFS, potential penalties under the False Claims Act, and reputational damage.
- **Possible Insurance Treatment**
- **Lessons Learned:** Be certain when certifying compliance, ask questions and have documentation, segment systems.

Possible Additional Causes of Potential Liability

Conduct in Regulatory Examinations

- Involvement in misconduct
- Withholding material information

Negligence in Data Handling or Collection (particularly relating to AI)

Compliance with GDPR (or similar privacy laws)

Allegations of Coverup

- Officers conceal the existence or severity of incidents or noncompliance

Insider Risks

- Insider incidents
- Collusion with criminals

Mitigation Strategies

Education and Training:

- Regular training on data protection laws and best practices.
- Awareness programs for employees.

Policies and Procedures:

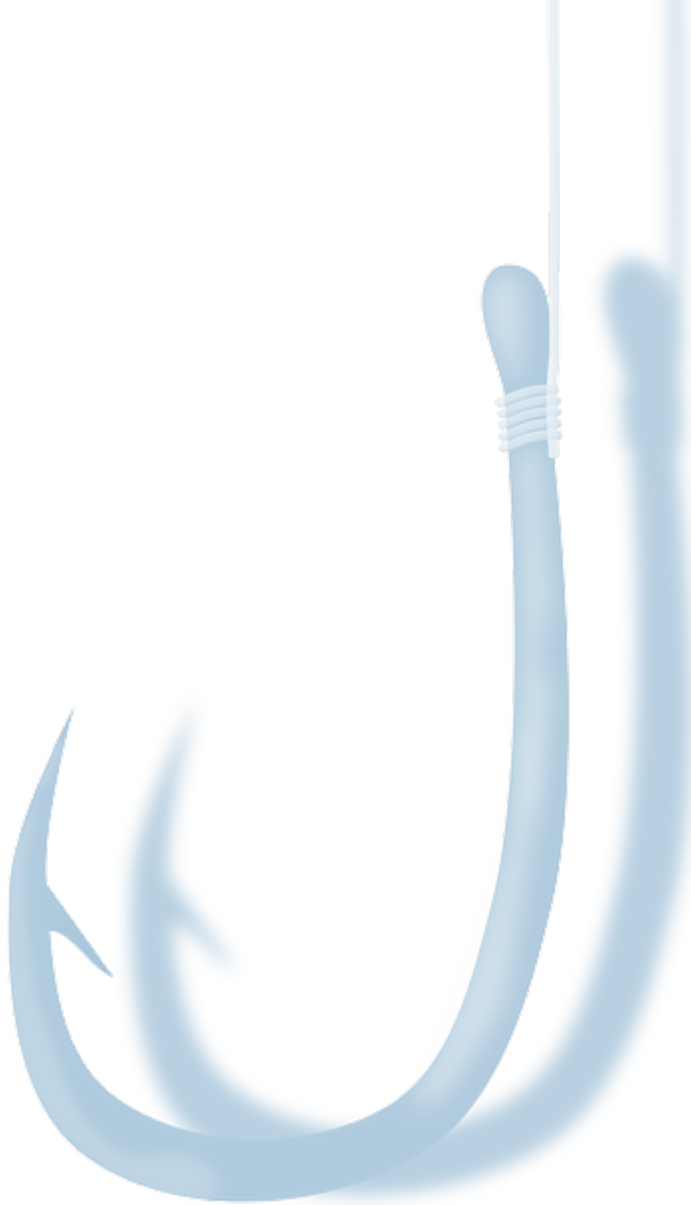
- Implementing comprehensive data protection policies.
- Regular audits and compliance checks.

Technical Measures:

- Encryption and access controls.
- Regular security assessments and updates.

Incident Response:

- Developing and testing incident response plans.
- Clear communication channels for reporting breaches.



Role of Legal Counsel

CONSULTATION

Regularly consult with legal experts to ensure compliance

DOCUMENTATION

Maintain thorough documentation of data protection efforts

LEGAL DEFENSE

Prepare for potential legal actions with a robust defense strategy.

troutman pepper locke

Best Practices for Data Guardians

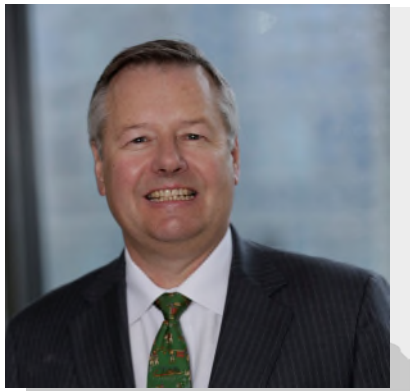
- **Proactive Approach:** Stay ahead of potential threats and regulatory changes.
- **Collaboration:** Work closely with IT, legal, and compliance teams.
- **Continuous Improvement:** Regularly update and improve data protection measures.

- **Summary:** Understanding personal liability and implementing mitigation strategies are crucial for data guardians.
- **Final Thoughts:** Proactive measures and continuous education are key to minimizing risks.

Questions

Ted Augustinos
Partner
Troutman Pepper Locke

Ryan Burch
Chief Privacy Officer
LPL Financial



Chris Keegan
Senior Managing Director
Brown & Brown

Lauren Roth
VP
Marsh USA

Jim Shreve
Partner
Troutman Pepper Locke

Thank You

Brown & Brown LPL Financial Marsh troutman pepper locke