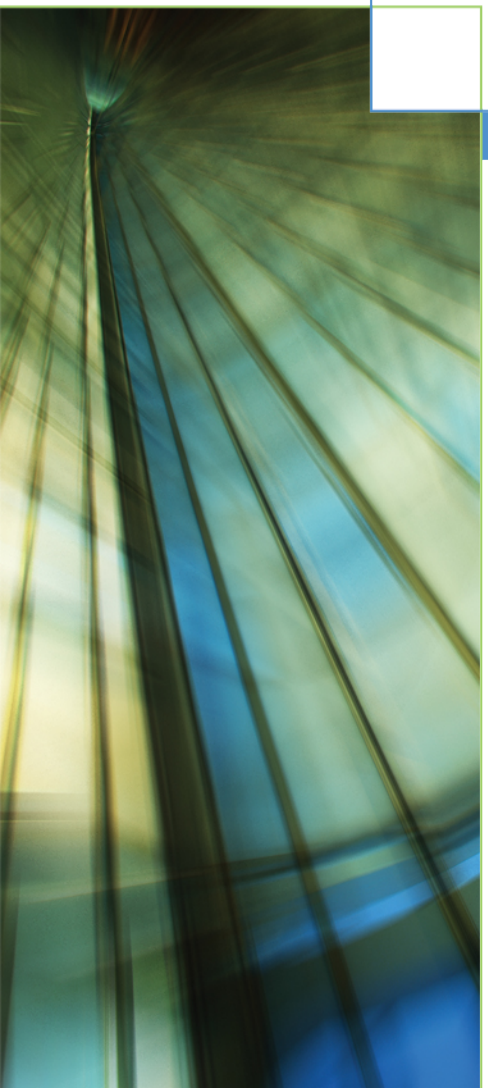
SILA FOUNDATION

Webinar: Cyber Security and Privacy

Thursday, Oct. 26 @ 3:00pm EST



Cybersecurity: Are You Prepared to Respond and Defend?

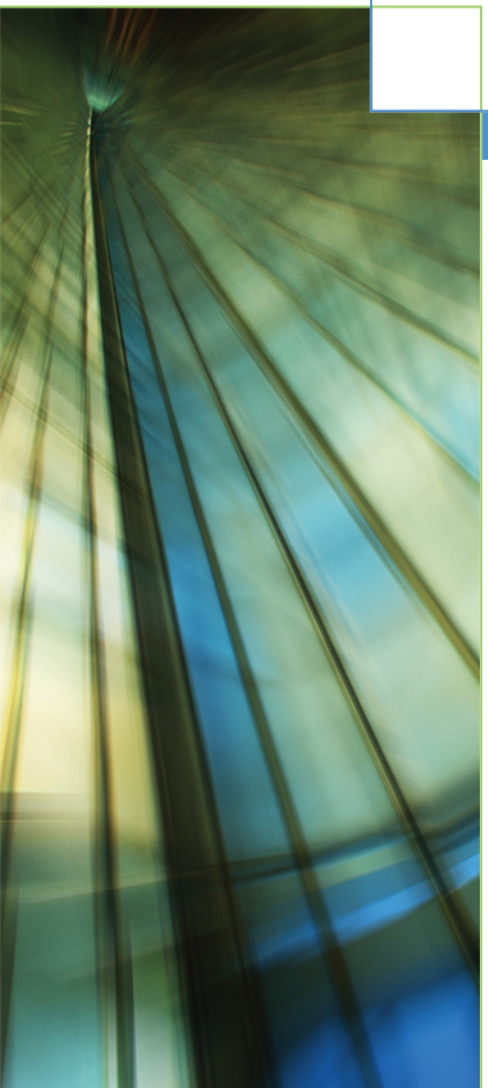
SILA Foundation Webinar October 26 , 2017

Lori Nugent
Shareholder
Cybersecurity, Privacy and Crisis Management

GT GreenbergTraurig

- Past the Tipping Point
- Responding Well Matters
- Are You Prepared Financially?
- Who Needs a Seat at the Table?
- What are Your Proof Points?
- Breach Scenarios to Consider

GT GreenbergTraurig



Past the Tipping Point

GT GreenbergTraurig

Cyber Crime is Big Business

- Cyber Crime is the FBI's #3 Priority
  - Behind Terrorism and Espionage
- Top Hackers Subcontract
- Regulators "Help" Companies Understand that Cyber Threats Require Attention

GT GreenbergTraurig

Disclosure Obligations

- Breach Notification Laws
  - 48 states (not South Dakota or Alabama) and D.C., Guam, Puerto Rico and USVI
  - Federal Regulations
  - Global Regulations (e.g. GDPR, Macao)

- Contractual Breach Notification Obligations
  - Vendor Management Contract Terms
  - Loan Covenant(s) and Other Private Agreements

GT GreenbergTraurig

Regulatory Hot Tin Roof

- Federal Agencies After OPM Breach
- State Regulator Coordination
  - Winning Since TJX Breach
    2009 Settlement by 41 AGs for $9.75 Million
- International Regulators' Scrutiny
  - Post-Snowden Mistrust
  - Different Values and Approaches
- **Regulators are Cash Positive**

GT GreenbergTraurig

Which Regulator is Most Aggressive?

- SEC
  - Sweeps
- FTC
  - Consent Decrees with Audits for 20 Years
- HHS
  - Hospice of Northern Idaho
- EU General Data Protection Regulation (GDPR)
  - Up to €20 Million or 4% of Annual Global Turnover
- State Attorneys General

GT GreenbergTraurig

State Regulators: Setting National Trends

- **California**
  - 2003 First Data Breach Notification Law
  - 2016 CA AG Adopted Center for Internet Security (CIS) Critical Security Controls
    Failure to Implement = “Lack of Reasonable Security”
- **Massachusetts**
  - 2007 Standards for Protection of Personal Information
    Requires encryption

New York

- 2017 Financial Services Regulation requires annual compliance certification, and breach notice within 72 hours

New York Department of Financial Services
Cyber Regulation and Enforcement

$2,500 potential fine per violation, per day the violation continues

$15,000 potential fine per violation, per day the violation continues for any reckless or unsound practice or pattern of misconduct

$75,000 potential fine per violation, per day the violation continues for a knowing and willful violation

GT GreenbergTraurig

Litigation Floodgates Opening

- **Standing:**

  Threatened Injury Certainly Impending and Fairly Traceable to Defendant

- **Sony:**
  - Wrongful Disclosure Causing Threat of Future Harm is Enough—No 3d Party Access Required

- **Neiman Marcus:**
  - Data Theft Necessarily Implies Imminent Threat of Harm Because Misuse of Data is the Purpose of a Breach

GT GreenbergTraurig

Class Action Standing

- *Neiman Marcus:*

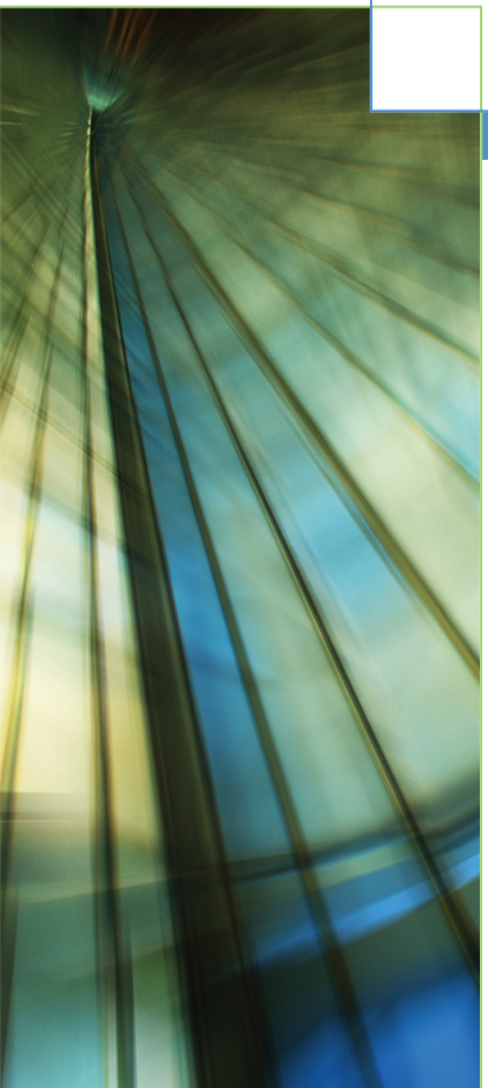
"At this stage in the litigation it is plausible to infer that plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach. Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."

GT GreenbergTraurig

Data Breach Class Action Claims:

- Negligence
- Breach of Contract
- Fraud
- Unfair Trade Practices/Consumer Protection
- Directors and Officers' Liability for Breach of Fiduciary Duty

Prepare for Defense on the Merits



Responding Well Matters

GT GreenbergTraurig

Responding Well Matters:

- Response Sets that Tone for:
  - Public Perception
  - Regulatory Investigation
  - Litigation
- Prepare to Act Quickly and Prudently to Protect:
  - Customers/Consumers
  - Shareholders and other Stakeholders
  - Brand
  - Cash Flow

GT GreenbergTraurig

What do Regulators Expect?

- Proof that Your Operation Isn't Careless, Including:

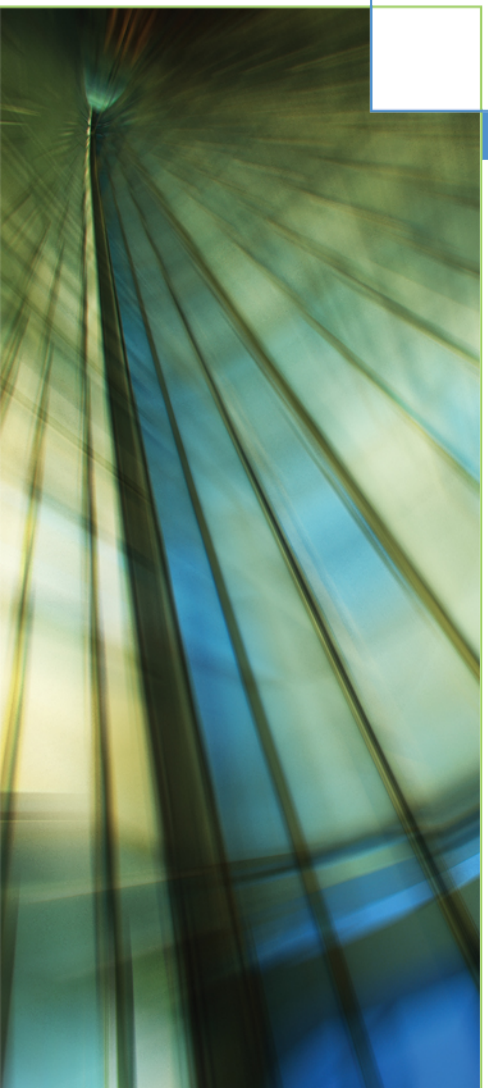
  - A Solid, Tested, Workable Breach Response Plan

  - Evidence that You:
    - Know What Sensitive Data You Handle,
    - Keep Only What it is Necessary, and
    - Take Reasonable Steps to Protect It

GT GreenbergTraurig

What do Regulators Expect?

- Timely Notification
- Quick, Accurate Count of the Number of Impacted Individuals Resident in Each Jurisdiction
- Clear, Fair Communication
- Services for Impacted Individuals



Are You Prepared Financially?

Average Cost of a Breach (2017)

- The average cost of a breach is $225/record
  - Not all records are created equal:
    - Health Care: $380/record
    - Financial: $336/record
    - Educational: $245/record
    - Retail: $177/record
- The average cost of a data breach in the USA is $7.35 million dollars

GT GreenbergTraurig

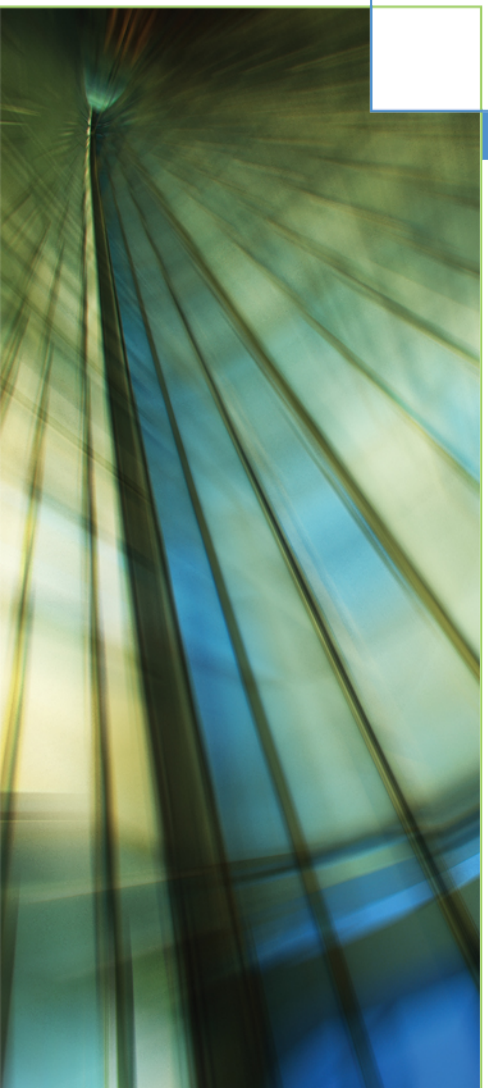
Are You Prepared Financially?

- Do You Know Your Maximum Probable Loss and Likely Frequent Losses?
  - Maximum Probable Loss
    - $225- $380 Per Impacted Individual
    - More Robust Valuation Using Breach Calculators
  - Frequency Valuation
    - Evaluate Prior Situations
    - Consider Impact of Mobile Technology
    - Don’t Forget Insider Risks and Vendors

GT GreenbergTraurig

Are You Prepared Financially?

- Are Your Cyber Reserves/Insurance Adequate?
  - Evaluated Annually
  - Based on MPL and Frequency Assessment
  - Supported by Independent Evaluation (e.g. Broker)
- Are Your Vendors' Reserves/Insurance Adequate if They Cause Your Loss? And Others on their Platform?
- Are You Satisfied with Contractual Joint Breach Response Requirements and Planning?



Who Needs a Seat at the Table?

GT GreenbergTraurig

Who Needs a Seat at the Table?

- Responding Well Requires an Enterprise-Level Plan
  - IT
  - Legal
  - Compliance
  - Finance
  - Risk Management
  - Human Resources
  - Public Relations
  - Each Operating Unit

GT GreenbergTraurig

Strong Incident Response Plans Include

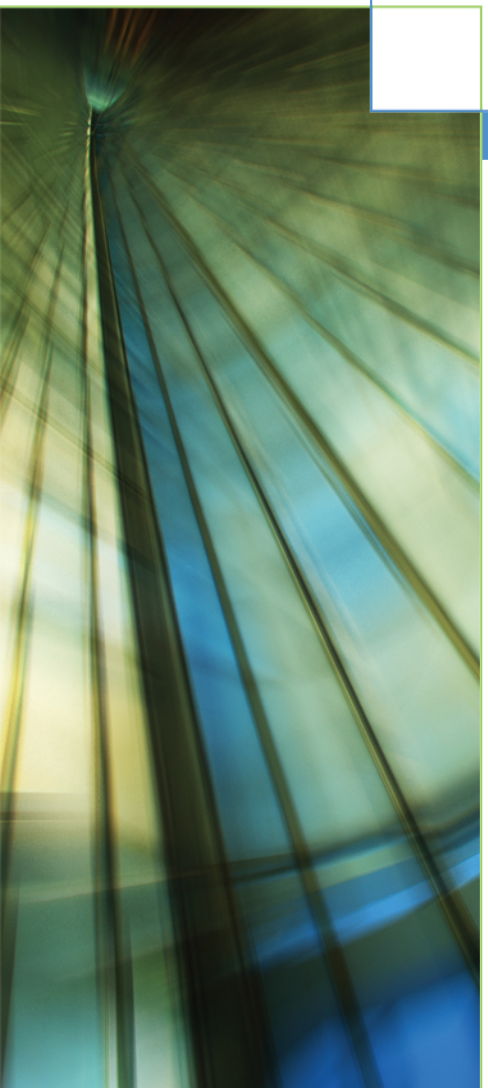
- Agreed Upon Authority and Roles
- Stakeholder Communication Plans
- Prudently Engaged Management and Board
- Trained Incident Response Team:
  - Reflects the Enterprise
  - Structured to Enhance Legal Protections
  - Includes Core Initial Investigation Team with Counsel
  - Preserves Evidence to Avoid Spoliation
  - Thoughtful Documentation

GT GreenbergTraurig

Preparing Incident Response Team Members

- Identify Individuals and Alternates
- Incident Response Team Members = Witnesses
- Choose Carefully and Confirm Readiness
- Train the Team
  - Know Who does What, When and Why
  - Agreed Upon Process and Authority
  - Method(s) for Keeping Stakeholders Informed
  - Appropriate Documentation

Preserve Evidence and Legal Protections while Avoiding Admissions



What are Your Proof Points?

GT GreenbergTraurig

What Evidence Proves Your Reasonableness to:

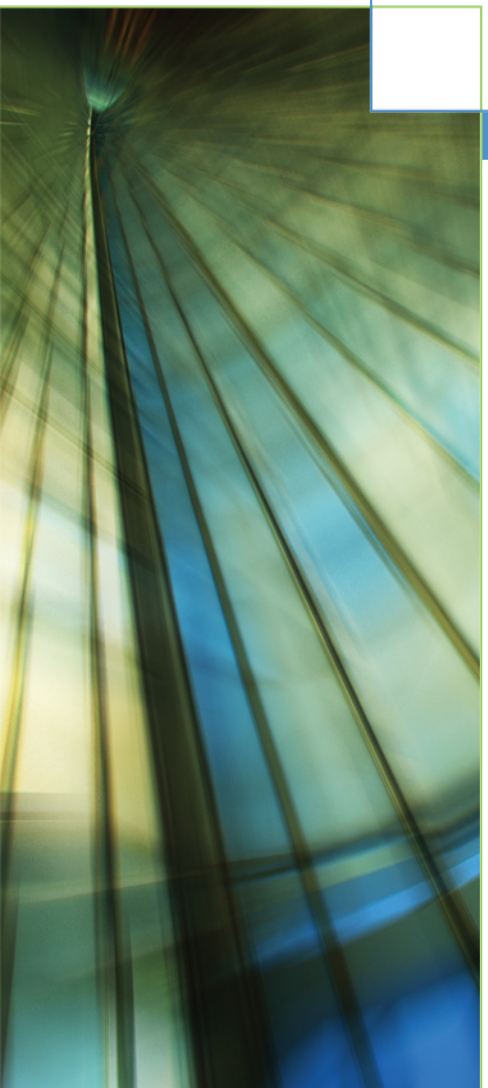
- Customers
- Business Partners
- Regulators
- Plaintiffs' Attorneys
- Shareholders
- Public

GT GreenbergTraurig

What are Your Proof Points?

- Defensible Positions
  - Maximize Legal Protection of Response
  - Preserve Evidence and Document Prudently
  - Strong Proof Points are Identified in Advance:
    - Active Management and Board Engagement
    - Reasonable Steps Taken to Minimize and Protect Sensitive Data Cradle to Grave
    - Appropriate Training and Testing
    - Independent Expert Validation of Good Practices
    - Key Documents and Witnesses are Ready

GT GreenbergTraurig



Breach Scenarios to Consider

GT GreenbergTraurig

Breach Scenarios to Consider

- Employee Data Breach
- Vendor's Breach of Your Customer Data
- Ransomware
- Social Engineering Induced Fraud
- Insider Compromise

What are Your Proof Points?

GT GreenbergTraurig

On the Horizon

- State AGs to continue aggressive regulatory actions
- Class action plaintiffs will benefit from regulatory activity
- Litigation costs and insurance premiums will increase as more courts find standing
- Malware and social engineering will continue to adapt to defensive efforts
- Continued nation-state and hactivist activity
- Legislative activity will continue to escalate
- Increasing complexity for cross-border data transfers

Questions?

GT GreenbergTraurig

Thank You!

Presented by:
Lori S. Nugent
Shareholder
Data Security, Privacy andCrisis Management
Greenberg Traurig, LLP
nugentl@gtlaw.com
224-279-5128