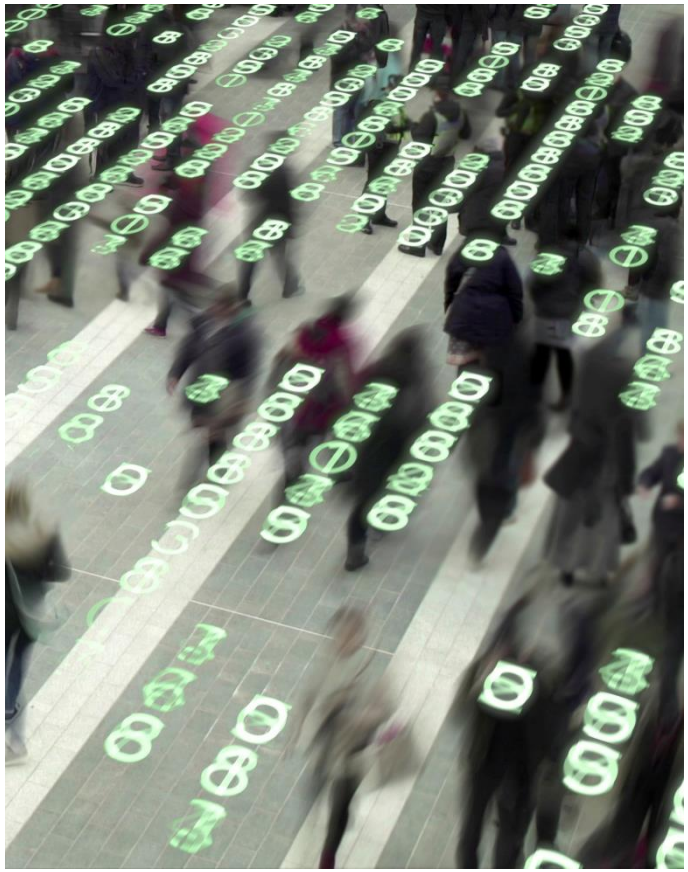
Victor O. Schinnerer & Company, Inc.

We're Under Cyberattack…Now What?!

John Mullen, Partner/Co-founder, Mullen Coughlin
Jason Bucher, Senior Underwriting Manager, Schinnerer Cyber Protection

Data Creates Duties

- **What data** do you access, and why?
- **Where** is it?
- How well is it protected?
- Who can access it? Why?
- When do you **purge it**?
- How do you purge it?



Threats

Malicious attack

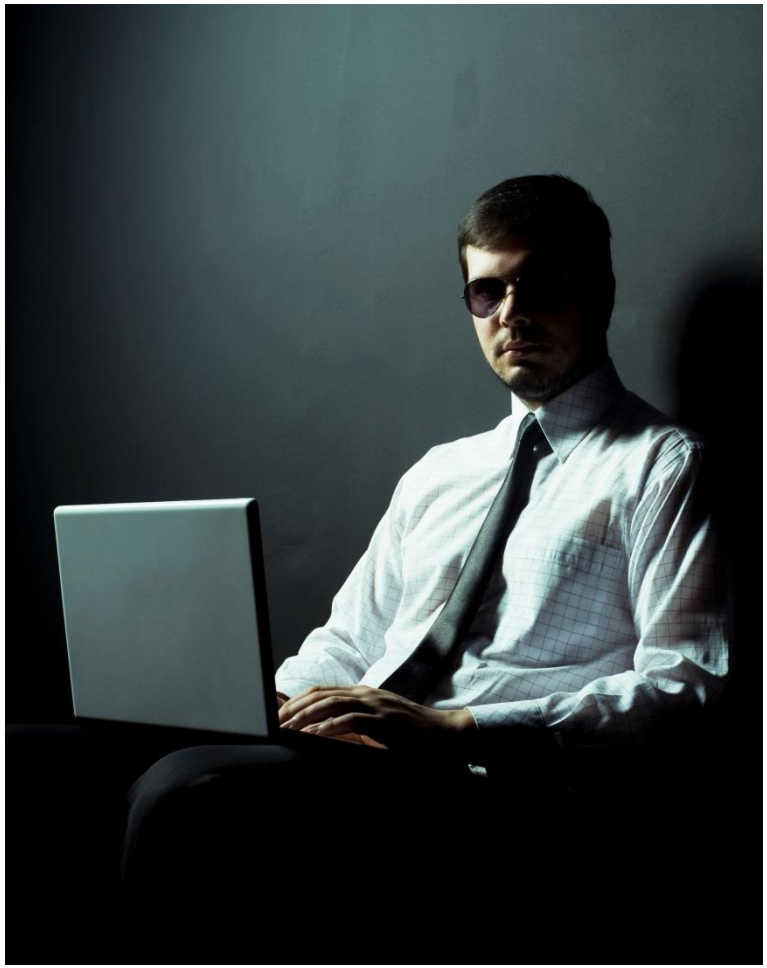
- **Hackers** in network, **malware** and viruses, **phishing** scams (ransomware), physical theft of hardware and paper
- **Rogue employees**

Employees

- **Negligence** related to use and storage of data, failure to follow or learn policies and procedures, loss of portable devices, mis-mailing of **paper**, unencrypted emails to the wrong recipients

Business partners

- Any of the above can occur to a business partner with whom data is shared

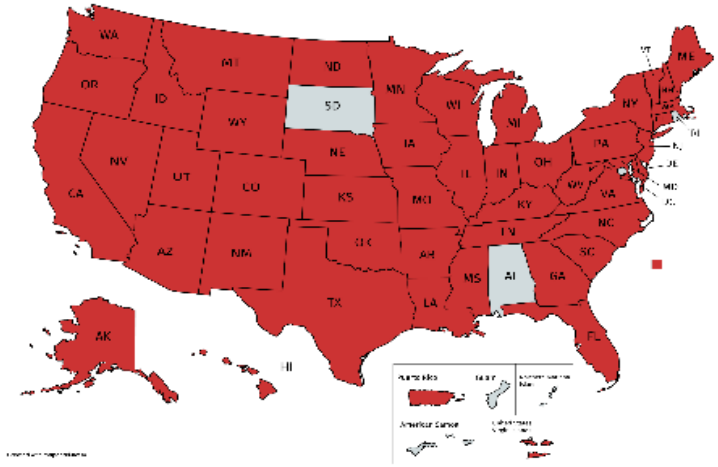


Ever Changing Definitions

- **Personally identifiable information (PII)** - i.e., Social Security number, driver's license number, bank account information, credit card information, online/financial account username and password, medical information, health insurance information, and email address and password
- **Protected health information (PHI)** - Information created or received by a covered entity or business associate **relating to the past, present or future physical or mental health** or condition of an individual; the provision of healthcare to an individual; or the past, present, or future **payment for** the provision of health care to an individual, that identifies or can be used to identify the individual
- **Payment card industry information (PCI**) - Cardholder data
- **Contracts**

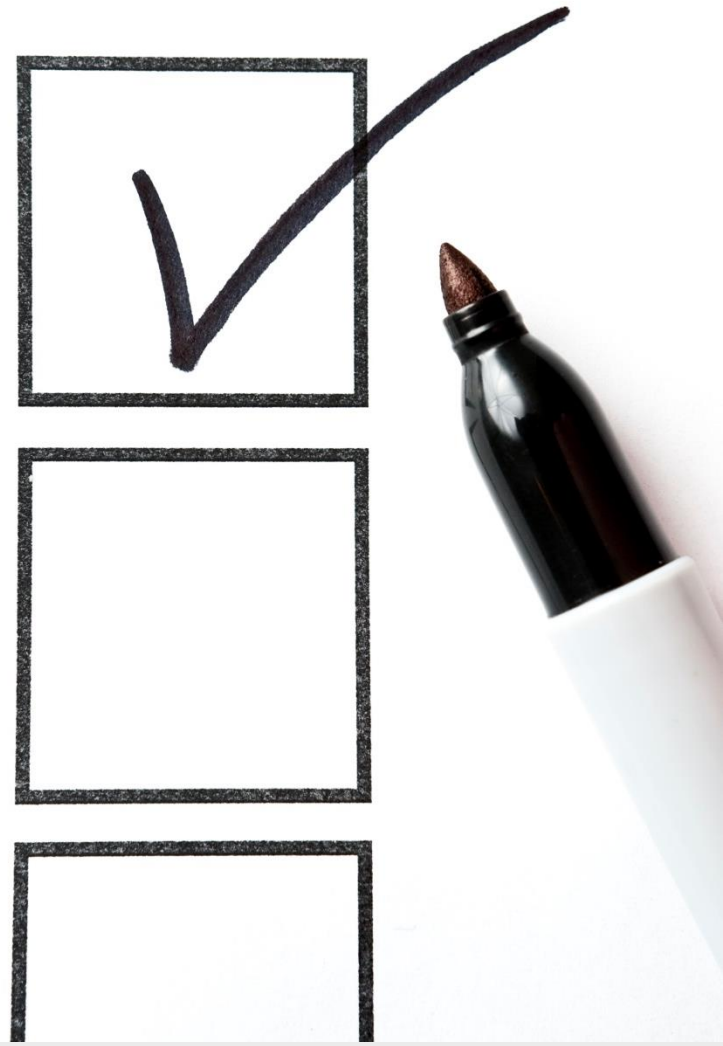
State Regulatory Exposures

- **48 states** (plus Puerto Rico, Washington D.C., Virgin Islands) require notice to residents after unauthorized access to personally identifiable information
- Require companies to **notify resident consumers** of security breaches of unencrypted computerized personal information (includes health information in some states)
- Many require notification of **state attorney general**, state consumer protection agencies, and credit monitoring agencies
- Notice due "**without unreasonable delay**", but some strict states (30/45/90 days)
- Some states are requesting an **Assurance of Voluntary Compliance**
- Some states allow **private right** of action for violations



Unwritten Rules

- Pennsylvania: (**AG likes notice** if incident affects significant number of PA residents, though no statutory requirement)
- California: (DHCS interprets California data breach statute to cover **paper** breaches, and expects CA legislature to update statute soon to clearly cover paper breaches)
- Indiana: (anything over **30 days** is "unreasonable delay")
- Connecticut: (**2 years** of credit monitoring) (90 days probably "unreasonable delay")

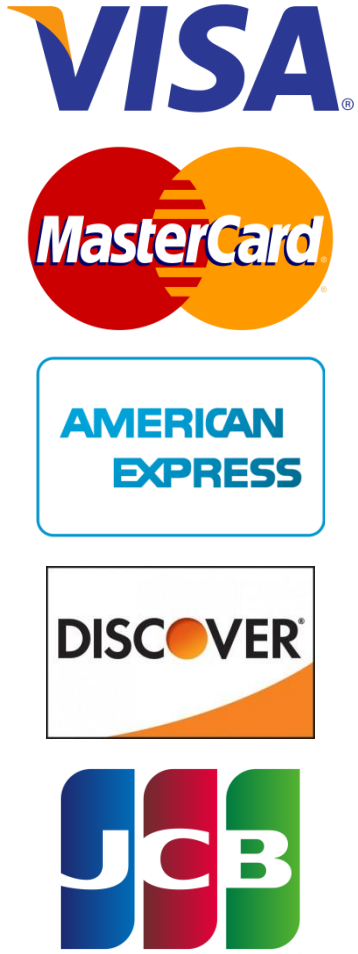


Federal Regulations

- July 7, 2015 - **47 State AGs write to Congress**, urging U.S. to preserve state authority over data breaches
- HIPAA/ HITECH
  - OCR **unofficially mandates** automatic investigation if over 500 affected
  - Covered Entities and their **Business Associates** subject to rules
- GLBA (Financial Institutions) - Privacy Rule suggests notification; Safeguards Rule suggests written security plan
- FERPA (Students) - Federal funding can be, but never has been cut off following violation
- SOX (Publicly Traded Companies) - Requires security controls, and auditors require disclosure if such controls are inadequate
- FACTA (Reuse of credit information) Red Flags Rule requires procedures to detect and prevent identity theft
- SEC (More aggressive cyber role expected)
- FTC
  - **Approx. 50 privacy investigations** since 2002, and dozens of fines ($22.5 million — Google 2012)
  - Actively enforcing health care vendor rules (breach reporting for non-HIPAA entities)
- FCC (Regulates communications networks)
  - **First ever data breach fine** (October 2014) ($10 million-TerraCom and YourTel America)

Payment Card Industry (PCI)

- Payment Card Industry Security Standards Council (Visa, MasterCard, AmEx, Discover, JCB International)
- Requires merchants and service providers to abide by certain protocols to protect customers' credit card information
- Imposes "assessments" and "fines" on offending merchants and service providers (can be millions)
- Violations of PCI DSS have multiple consequences
- Impact on standard of care — industry investigations, outside lawsuits
- Small minority of states have incorporated PCI-DSS requirements into data protection laws
- **Privileged forensics vs PFI**



Anatomy of a Breach Response

BREACH DISCOVERY

EXPERTS
- Breach coach
- Forensics
- Public relations

INVESTIGATION - internal/forensic/criminal
- How did it happen?
- When did it happen?
- Is it still happening?
- Who did it happen to?
- What was accessed/acquired? (What wasn't?)

NOTICE OBLIGATIONS
- State
- Federal
- Other (i.e. PCI)
- Deadlines – Can be 48 hours

NOTIFICATION

PROCESS
- Written
- Electronic
- Substitute
- To Media

VENDORS
- Printing, Mailing and Call Center
- Credit Monitoring

INQUIRIES
- State Regulators (i.e. AG, PD)
- Federal Regulators (i.e. OCR)
- Federal Agencies (i.e. SEC, FTC)
- Consumer reporting agencies
- Potential Plaintiffs

LITIGATION
- Government Entities
- Class Action
- Indemnification

Data Breach Litigation

- Federal jurisdictions that have found **Article III standing in the absence of identity theft**:
  - Sixth Circuit
    - Galaria et al. v. Nationwide Mutual Insurance Company No. 15-3387, 2016 WL 4728027 (6th Cir. September 12, 2016)
  - Seventh Circuit
    - Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688 (7th Cir. 2015)
  - Eighth Circuit
    - Kuhns v. Scottrade, Inc., No. 16-3426, No. 16-3542, 2017 WL 3584046 (8th Cir. Aug. 21, 2017) (dismissed on other grounds)
  - Ninth Circuit
    - Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010)

Data Breach Litigation – Settlements

- In re Anthem Inc. Data Breach Litigation, 5:15-md-02617 (N.D. Ca.)
  - *Pending Court Approval*
  - Settlement valued at **$115 million** to end litigation over 2015 data breach affecting approximately 80 million
  - Settlement includes an **additional two years of credit monitoring** available to the individuals involved in the breach **or** alternative cash compensation to those already enrolled with credit monitoring services
  - $15 million of settlement dedicated to **pay certain out-of-pocket expenses** class members incurred
- Remijas et al. v. the Neiman Marcus Group LLC, 1:14-cv-01735 (N.D. Ill)
  - **$1.6 settlement** between Nieman Marcus and a class of customers whose credit card data was exposed in 2013 data breach
  - Approximately **370,385 cards** were used during a three month window in which card-scraping malware was operating on the company's computer system
  - Customers who file a claim showing their card was used during the window will receive **$100**

Best Practices Pre Incident

- **Empower** Senior Executives
- **Talk** to your IT Security folks. Gain an appreciation of the many challenges and risk landscape
  - Not many Firms can say: how many records they have; what type of data is being collected, stored, shared, protected; where does all this data reside; when is it purged?
- **Assess and test** your own staff and operations
- **Prepare and test** incident response plan
- **Document** your due care measures (training and enforcement)
- **Secure** appropriate insurance
- **Execute** service level agreements – **manage your vendors**
- Repeat

Best Practices Post Incident

- **Ensure experience** on Response Team
  - Post data incident is not the time to learn the ins and outs of incident response
  - Establish **Incident Response Team** of decision-makers (if not established already) as things move too fast for typical bureaucracy

- Use Counsel to Establish **Privilege**
  - Counsel directs forensics, notice drafting, and other vendors so that, in the event of litigation or regulatory investigation, all documents and communications are not discoverable
  - Guard Attorney-Client Privilege: **do not** share forensic reports, legal analysis and drafts with clients or third parties if not absolutely necessary

Best Practices Post Incident

- Do not **use terms "Breach" or "PII" or "PHI" lightly** — these are statutorily defined legal terms the use and admission of which have consequences
- Do not rush to go public
  - Tremendous desire to go public fast, but an inability to answer questions that will inevitably follow can be devastating
  - **If you notify 4 hours after discovery there will be people who charge you with delay, so "delay" is unavoidable**
- **Prepare for litigation** and regulatory investigation — Preserve all relevant documents
- Conduct risk assessment and implement **data security improvements** prior to being asked by a regulator

Your Schinnerer Cyber Team

Jason Bucher
Senior Cyber Underwriter
Phone: (913) 685-6166
jason.bucher@schinnerer.com

Zach Atya
Cyber Assistant Account Executive
Phone: (301) 961-9893
Zacharia.Atya@schinnerer.com

Mark Schulz
Cyber Underwriter
Phone: (860) 723-5663
Mark.Schulz@schinnerer.com


Questions?


Victor O.
Schinnerer
& Company, Inc.


MC