A PRIMER ON U.S. PRIVACY AND SECURITY LAW

Tsutomu L. Johnson and J. Michael Bailey

September 7, 2018

PARSONS BEHLE & LATIMER

What is Regulated Information

- Personally Identifiable Information: A person's first name or initial, plus their last name, and one of the following:
  - Social Security number;
  - Financial account number, or credit or debit card number and a security code or password to access the account; and
  - Driver license number or state ID card number.

PARSONS BEHLE & LATIMER

What is Regulated Information

- Protected Health Information:
  - Any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity.
  - If your organization has signed a Business Associate Agreement, you must follow the HIPAA and HITECH privacy and security rules.
  - Even if your company isn't a Covered Entity it may sponsor a group health insurance plan for its employees. If so, it may need to comply with parts of the HIPAA privcy rule.

PARSONS BEHLE & LATIMER

What is Regulated Information

- Nonpublic Personal Information:
  - Any information: an individual gives a Financial Institution for a financial product or service; a financial institution receives about an individual from a transaction involving the financial institution's products; or a financial institution gets about an individual in connection with providing a financial product or service.
  - Financial Institution: an organization that is significantly engaged in financial activities.
  - Safeguards Rule: Sets privacy rules for Financial Institutions to assess risk, create organizational safeguards, respond to incidents, and oversee service providers.

PARSONS BEHLE & LATIMER

What's Going On?!

- Increased Federal Regulation
  - FCC: In 2015, the FCC issued millions in fines for the loss or unauthorized access of Consumer Proprietary Network Information.
  - FTC: Third Circuit approves FTC's "authority to regulate cybersecurity under the unfairness prong of 15 USC § 45(a)"
  - Office of Civil Rights: Levied more than $14M in fines this year against companies for losing health information, failing to have the appropriate contracts to protect health information, and for failing to timely respond to security events.

PARSONS BEHLE & LATIMER

What's Going On?!

- Increased State Regulation
  - For example, under Utah Code Ann. § 13-44-201 (1), "Any person who conducts business in the state and maintains personal information shall implement and maintain reasonable procedures to: (a) prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business . . . ."

PARSONS BEHLE & LATIMER

What's Going On?!

- Commercial contracts require:
  - Compliance with "industry security standards" such as ISO, NIST, and PCI;
  - Compliance with federal and state security and privacy standards even if you aren't a regulated entity;
  - Guarantees that your privacy and security program prevents all incidents;
  - Random audits; and
  - Unbound liability for failing to deliver on your privacy and security promises.

PARSONS BEHLE & LATIMER

What's Going On?!

- Executive and Board Member liability:
  - Executives and board members have a duty of loyalty and duty of care to the companies they manage:
    - Duty of Care: Executives and board members must act on an informed basis and must act reasonably to assess and address security and privacy risks.
  - Important notes:
    - A breach of the duty of care can create personal liability.
    - In some states, a breach of these fiduciary duties can result in punitive damages, which may be uninsurable.
    - CGL policies don't cover directors and officers, and D&O policies generally don't cover data breach events. You either need a broad E&O policy or a cybersecurity and privacy addition to your CGL policy.
  - Example: After the Home Depot data breach in 2014, the shareholders proposed a settlement requiring:
    - About $1.2M in attorney fees.
    - Stronger board oversight of the CISO.
    - Enhanced security programs, exercises, and training validating security processes and procedures.

PARSONS BEHLE & LATIMER

How Do I Address this Problem?

- Generally, businesses need to implement technical and organizational privacy and security policies that reasonably protect the confidentiality, integrity, and accessibility of information.

PARSONS BEHLE & LATIMER

How Do I Address this Problem?

- Approaching the problem:
  - Identify legal obligations
    - Review industry regulations, contractual obligations, and general security/privacy regulations.
  - Examine the environment
    - Evaluate how information flows through the organization, how it's manipulated, whether the organization assigns security protocols to that information, and how the information is deleted.
  - Address legal risks:
    - Create a Privacy Policy that addresses legal risks.

PARSONS BEHLE & LATIMER

How Do I Address this Problem?

- What you need:
  - Processes that report privacy and security initiatives, incidents, and training levels to the board and relevant executives.
  - An organizational chart clearly showing which executives and board members (or committees) are responsible for privacy and security. The chart should explain how the company divides privacy, security, audits, and incident response tasks.
  - Policies explaining how the organization tracks information, manages information, and deletes information.
  - Contracting procedures for handling Personal Information.
  - Security Procedures and Controls to reasonably protect the organization.

PARSONS BEHLE & LATIMER

Reporting Processes

- Create a Privacy Office that reports privacy and security compliance, incidents, and audits executive stakeholders and the Board of Directors.
- The Privacy Office should oversee:
  - Privacy initiatives and compliance,
  - Security initiatives and compliance,
  - Incident response tasks,
  - Privacy by design initiatives,
  - Training programs, and
  - Audits of the privacy and security program.

PARSONS BEHLE & LATIMER

Privacy and Security Policies

Privacy Policies	Security Policies
Establish the Privacy Office	Set a framework: - CIS 20 CC, - ISO 27001, - NIST Cybersecurity Framework
Set the reporting hierarchy for the Privacy Office	Determine framework obligations
Include the following policies and procedures: - Notice, Transparency, and Consent - Purpose Limitation and Data Minimization - Legal Basis for Processing - Subcontracting - Data Transfers - Record of Processing - Data Protection, Security Measures, and Physical Security	Incorporate framework into policies Create procedures to achieve policy goals Create controls to demonstrate evidentiary compliance with security procedures

PARSONS BEHLE & LATIMER

Incident Response

- Create an incident response process that:
  - Sets the flow for discovering incidents, reporting incidents, and recovering from incidents.
  - Describes who coordinates incidents and who sits on the incident response team.
  - Utilizes a standard incident report form that summarizes the incident, keeps a timeline of the incident, identifies root causes, and details remediation efforts.

PARSONS BEHLE & LATIMER

What Should You Do?

- When you get back to your office:
  - See if you have a privacy or security policy. If you don't, call us and we can sit down for a free consult.
  - Call your insurance agent and make sure you are covered for security and privacy events.
- In the next 30 days:
  - Align key stakeholders in executive management to setup a privacy and security program.
  - Assess legal risks.
  - Establish an incident response process.
- In the next quarter:
  - Set privacy and security policies and procedures.
- In the next year:
  - Audit the privacy and security program to make sure it achieves its goals.
  - Start a training program.
  - Create an "essential" privacy and security program for employees that distills the privacy and security program for employees.

PARSONS BEHLE & LATIMER

Thank You

- If you have any questions, or need a free copy of security procedures and controls, please contact me at:

Tsutomu Johnson
Tjohnson@parsonsbehle.com
801.536.6903

J. Michael Bailey
mbailey@parsonsbehle.com
801.536.6777

PARSONS BEHLE & LATIMER

Disclaimer

- The slides contained herein and the content they contain are for informational purposes only and not for the purpose of providing legal advice. You should not rely on the information contained herein without seeking the advice of an attorney. Reviewing or receiving these slides does not create an attorney client relationship between you and Parsons Behle & Latimer. For any particular legal issue or problem, you should contact an attorney directly to obtain legal advice.

PARSONS BEHLE & LATIMER