DCIA Annual Forum
May 15, 2018

The Ever Changing Cyber Regulatory Landscape - Where are we now?

Brian T. Robb
Cyber Industry Leader
CNA Insurance

Agenda

- State Regulations
  - Review of Delaware's Breach Notification Law
  - NYS DFS Regulation
- Federal Regulation
  - Review of the regulations and agencies
  - Review of enforcement
- European General Data Protection Regulation
  - Overview
  - What does it mean for US based companies
- Payment Card Industry
  - PCI Compliance
  - Fines and Assessments

Current Regulatory Landscape

The only certain thing is uncertainty!

State Regulations

- All 50 States have Data Breach Laws
- In general, these laws cover
  - When and how to notify Consumers
  - Notification obligations to State AG's
  - If there is an Encryption Safe Harbor
  - What constitutes Personally Identifiable Information (PII)
- However, each State data breach law is unique
- If a company has clients in multiple states, it will need to be aware of the different state laws that may apply if they suffer a breach

State Regulatory Authority and Enforcement

Delaware

- What is covered/ scope?
  - an individual's name along with:
  - (1) a Social Security number,
  - (2) a driver's license or government id card number,
  - (3) a credit card, debit card, or account number in combination with any required security code, access code, or password,
  - (4) a passport number,
  - (5) a username or email address, in combination with a password or security question, (6) an individual's medical history, treatment, diagnosis, or DNA profile,
  - (7) a health insurance policy number or other unique identifier used by a health insurer, (8) unique biometric data generated for authentication purposes, or
  - (9) an individual taxpayer identification number.

State Regulatory Authority and Enforcement

Delaware

- Who has to be notified?
  - Notification is required if an entity determines that a breach compromises the security, confidentiality, and integrity of personal information. Notification is required once a breach occurs unless the entity conducts an appropriate investigation and reasonably determines that the breach is unlikely to result in harm to affected individuals.
  - Notification to affected individuals must occur within 60 days of the determination that a breach occurred
  - Delaware AG no later than affected individuals if over 500 people
- An entity must provide credit monitoring services for at least one year to any individuals whose Social Security numbers were compromised, or reasonably believed to have been compromised, as the result of a data breach.
- Encryption Safe Harbor exists, unless the encryption key is also breached

State Regulations

- New York Department of Financial Services (NYDFS)
  - March 2017 – Cybersecurity Requirements
  - Impacts every bank, insurer, financial entity and third party service providers to those entities governed by the NYDFS

State Regulations

NYDFS Regulations Cont.

- Adapts Industry Best Practices – 23 Sections

8 Key Implementations
Mandatory Chief Information Security Officer
Periodic Testing
Reporting within 72 Hours of an Event
Limiting Access
Training
Written Plan
Encryption
Third Party Service Provider Risks

State Regulations

Other Potential State Regulations

- NYDFS regulations are a model
- National Association of Insurance Commissioners (NAIC) is set to release their final draft of a model cyber security law
- Many States have indicated that they are considering different cybersecurity legislation

Federal Regulations & Agencies

Industry Sector	REGULATIONS
Healthcare	HIPPA
	HITECH
Financial	FCRA
	FACTA
	GLBA
Education	FERPA
Marketing	CAN SPAM
	DNC

AGENCIES
FTC
FCC
HHS
DHS
DOT
SEC
OCR

Federal Regulatory Authority and Enforcement

Heathcare Sector

- OCR, HHS
- Involved with HIPAA, HITECH, GINA

Important Terms:

- PHI – Protected Health Information
- E-PHI – Electronic Protected Health Information

GINA
GENETIC INFORMATION NONDISCRIMINATION ACT

HIPAA

DEPARTMENT OF HEALTH & HUMAN SERVICES • USA

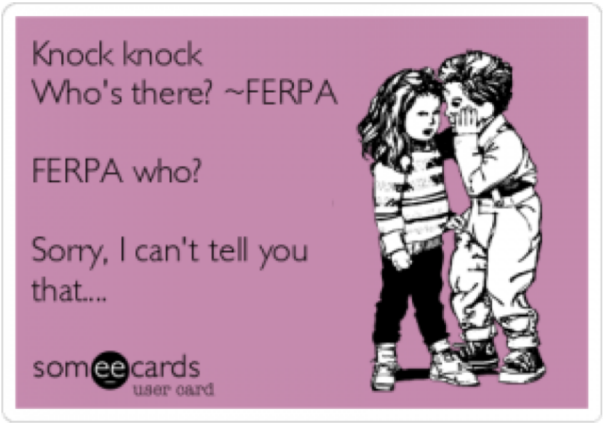
Federal Regulatory Authority and Enforcement

Educational Sector

- OCR
- Involved with FERPA, PPRA

Important Terms:

- "Educational Records"



Federal Regulatory Authority and Enforcement

Financial Sector

- FTC, SEC, also State A.G.
- Involved with FCRA, FACTA, GLBA

Important Terms:

- CRA – Consumer (credit) reporting agencies
- “Financial Institutions”

Federal Regulatory Authority and Enforcement

- Gramm-Leach-Bliley Act
  - Financial institutions are required to:
    - Store personal financial info. in a secure manner
    - Provide notice of their policies regarding sharing
    - Provide consumers with the choice to opt-out of sharing some information

Federal Regulatory Authority and Enforcement

- Gramm-Leach-Bliley Act
  - Enforced by:
    - FTC
    - SEC
    - State Agencies
  - Penalties for Violations
    - Up to $100,000 for each violation
    - Officers and Directors can be fined up to $10,000 per violation
    - Criminal penalties – 5 years, + fines

Federal Regulatory Authority and Enforcement

Retail and Marketing Sectors

- FTC, FCC
- Oversees CAN- SPAM, TSR
  - See also: Telecommunications Act of 96,
  - Cable Television Privacy Act of 84,
  - Video Privacy Protection Act of 88

Important Terms:

- Telemarketing
- Existing Business Relationship

NATIONAL
DO NOT CALL
REGISTRY

Federal Regulatory Authority and Enforcement

- Dodd-Frank Wall Street Reform and Consumer Protection Act
  - Created the Consumer Financial Protection Bureau (CFPB)
    - Bureau is tasked with promoting fairness and transparency for financial products
  - Enforced by CFPB, FTC, SEC
    - Federal Reserve has rule making authority
  - Penalties:
    - Max $5k for Tier 1 violations; $27k for Tier 2 violations, and $1,000,000 for Tier 3

Federal Regulatory Authority and Enforcement

- Fair Credit Reporting Act
  - Mandates accurate and relevant data collection
  - Consumers must be provided access to their information
  - Limits the use of consumer reports to defined purposes
  - Enforced by the FTC and State Attorneys General
  - Penalties:
    - Nominal, actual, or punitive damages
    - Criminal

European Union General Data Protection Regulation (GDPR)

- The GDPR goes into effect on May 25, 2018 – and there's no additional grace period.
- Some Key Points:
  - Directly covers many more companies and activities
  - Extends long-arm jurisdiction
  - Sky-high fines authorized . . . for just about everything
  - Consent is no longer a cure-all
  - Breach notification requirements
  - Many companies required to appoint data protection officers
  - Well-funded, powerful national data protection authorities
  - And a new central EU bureaucracy to oversee it all

European Union General Data Protection Regulation (GDPR)

- Does the GDPR Apply to your organization?
- Companies with an "establishment" in the EU are subject to the Regulation, ***regardless of where they process personal data***. That means that cloud-based processing performed outside of the EEA for an EEA-based company is covered by the Regulation.
- Non-EU companies that ***monitor the behavior*** of data subjects in the EEA (e.g., profiling; behavioral advertising).
  - Generally, will need to appoint a representative in the EU.
- Non-EU companies that ***offer services or goods*** to data subjects in the EU (including for free . . . like app providers)
  - Generally, will need to appoint a representative in the EU.
- New: Data processors as well as data controllers are directly liable under the Regulation.

European Union General Data Protection Regulation (GDPR)

- Who and what is protected by the GDPR?
- The Regulation protects living “natural persons, whatever their nationality or place of residence.”
- The data subject does not need to be an EU citizen or resident.
- Personal data is defined as "any information relating to an ***identified or identifiable*** natural person . . .”
  - Device identifiers and IP addresses usually will be personal data.
  - Publicly available information is still personal data
- Special/sensitive personal data: Biometric data and genetic data have been added to the current categories: data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health, sex life or sexual orientation

European Union General Data Protection Regulation (GDPR)

- What are the obligations if there's a data breach?
- Controller must report personal data breaches to DPA within 72 hours (where "feasible") of becoming aware of the breach, unless controller can demonstrate "that the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals."
  - If reporting is required but cannot be done within the 72 hour time limit, the controller must explain why it couldn't report on time.
- Breaches must be disclosed to the affected individuals "without undue delay if the personal data breach is likely to result in a high risk" to their "rights and freedoms."
- Processor must report breach to controller "without undue delay."
  - Contracts between controllers and processors will need to be more precise than that!

European Union General Data Protection Regulation (GDPR)

- What are the ***FINES***?
- Maximum fines of the higher of €10,000,000 or 2% of group's worldwide turnover (i.e., global gross revenue), for a long list of violations ranging from failure to implement privacy by design to failing to give notice of data breaches
- Maximum fines of the higher of €20,000,000 or 4% of group's worldwide turnover for violations of the rights of data subjects, including the "basic principles" for processing, non-compliant data transfers, and failure to comply with DPA orders
- For most purposes, companies should assume that fines would be based on their corporate group's worldwide revenue.

Other Regulations

Payment Card Industry

"PCI"

PCI 3.2

- What is PCI (industry standard, not a “law”)
- Level’s 1-4, only level one has a third party audit
- Yearly PCI compliance
- Version 3.1 expired on 31 October 2016
- All new requirements are best practice until February 2018
  - Validate security controls following a change in cardholder data environment
  - Perform penetration testing on segmentation controls every six months
  - Multi-factor authentication for Admin access
  - Perform quarterly reviews to confirm that personnel are following security policies

Questions

???

Brian T. Robb
Underwriting Director
Cyber Industry Leader
Brian.Robb@cna.com
212-440-3018