



BakerHostetler

Internal Controls and Compliance

Will Daugherty – Counsel, BakerHostetler
John DeLozier – Principal Consultant, Mandiant

Introductions – Mandiant & BakerHostetler



- Trusted Partner to Organizations Worldwide
Expert Responders to Critical Security Incidents
- True Thought Leaders
- Assist With All Stages of Incident Response and Preparedness
- Global footprint with over 300 consultants worldwide

BakerHostetler

- Chambers USA nationally ranked Privacy and Data Protection practice
- Privacy and Data Protection “Practice Group of the Year” by Law360 (2013 – 2016)
- Over 2,100 incidents handled (450+ in 2016 alone)
- Team includes 40+ attorneys specializing in privacy and data security law across the country

Agenda

- Data Security and Privacy Laws and Standards
- Security Frameworks
- Implementing a Security Program
- Prioritizing Security Controls

Data Security and Privacy Laws and Standards

Federal Data Security Laws

State Data Security Laws

Industry Self-Regulation & Guidelines

International Laws

Federal Privacy / Data Security Laws

Gramm Leach Bliley Act (GLBA)

[\[codified within 15 U.S.C. §§ 6701-81, 6801-27, 6901-10 and elsewhere\]](#)

- **Privacy Rule:** Requires disclosure to consumers and customers of how information is collected, shared, and protected.
- **Safeguards Rule:** Requires development, implementation and maintenance of written comprehensive information security program.

HIPAA / HITECH

[\[https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996\]](https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996)

- **Privacy Rule:** Requirements for use and disclosure of "PHI" by "covered entities" and "business associates".
- **Security Rule:** Establishes administrative, technical, and physical security standards for protection of e-PHI.

FTC Act – Section 5 and FTC Enforcement

- Section 5 of the FTC Act prohibits "**unfair or deceptive acts or practices** in or affecting commerce."
- The FTC has alleged that companies who fail to protect data after promising to do so have acted **deceptively**.
- The FTC has brought enforcement actions for failure to employ "**reasonable security measures**" to protect consumers' personal information as **unfair business practice**. (e.g., In re LabMD)



BakerHostetler

State Data Security Laws

Reasonable Security Procedures

- Several states require entities to "**implement and maintain reasonable security procedures**" to protect personal information, but without specifying particular safeguards or practices. E.g., Ark. Code Ann. §4-110-104(b); Cal. Civ. Code § 1798.81.5; Tex. Bus. & Com. Code § 521.052.

Massachusetts (201 CMR 17.00 et seq.)

- Implement and maintain **physical, administrative and technical information security measures** to safeguard personal information.
- Maintain a "**written comprehensive information security program**" that contains specific security requirements (access control protocols; encryption of PII; firewalls; A/V)
- Designate employee to maintain WISP



BakerHostetler

Find the full text of this and thousands of other resources from leading experts in dozens of legal practice areas in the [UT Law CLE eLibrary \(utcle.org/elibrary\)](http://utcle.org/elibrary)

Title search: Internal Controls and Compliance

Also available as part of the eCourse

[Preventing, Detecting, and Responding to a Data Breach: Internal Controls and Compliance](#)

First appeared as part of the conference materials for the
2017 Essential Cybersecurity Law session
"Internal Controls and Compliance"