MANDIANT
A FireEye® Company

BakerHostetler

# Internal Controls and Compliance

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

# Introductions – Mandiant & BakerHostetler

MANDIANT
A FireEye® Company

- 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 2014 and 2015 nationally ranked Privacy and Data Protection practice
- Privacy and Data Protection "Practice Group of the Year" by Law360 in 2013, 2014, & 2015
- Over 1,300 incidents handled (300+ in 2015 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
- Regulator Hot Buttons

MANDIANT A FireEye® Company

BakerHostetler

# Data Security and Privacy Laws and Standards

- Federal Data Security Laws
- State Data Security Laws
- Industry Self-Regulation & Guidelines
- International Laws

MANDIANT A FireEye® Company

BakerHostetler

# 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)

## FTC Act – Section 5 and FTC Enforcement

MANDIANT
A FireEye® Company

BakerHostetler

# 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)

- **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

MANDIANT
A FireEye® Company

BakerHostetler

# Title search: Internal Controls and Compliance



First appeared as part of the conference materials for the
2016 Essential Cybersecurity Law session
"Internal Controls and Compliance"