KING & SPALDING

Data, Privacy and Security Practice

As security incidents and issues related to data privacy become more prevalent, many companies need to prepare, respond, and recover. Is your company prepared?

CYBERSECURITY LANDSCAPE[1]

Facing an increasingly sophisticated and dynamic cyber threat landscape, executive management and corporate boards must be able to understand and address the ongoing legal challenges of protecting data; satisfying the multi-faceted regulatory controls on data use, access, and sharing; and conducting the appropriately scoped diligence for contemplated corporate transactions. The number of reported breaches continues to trend upward, with 2017 seeing a record high number of reported data breaches in the U.S., representing a 47% increase from 2016. Hacking is the most prevalent attack vector, accounting for nearly 60% of all breaches in 2017. The preliminary 2018 figures appear similarly daunting.

[1]***Sources:*** *2017 Data Breach Year-End Review and IBM X-Force Threat Intelligence Index 2018 released by the Identity Theft Resource Center and CyberScout*

HOW WE CAN HELP

Proactive Counseling

- Develop incident response plans and legal playbooks
- Advise executives and board members on cybersecurity oversight
- Conduct cybersecurity table-top exercises
- Counsel on international data breach laws
- Advise on implications of international data transfers
- Conduct global privacy impact assessments, including GDPR and data protection laws
- Conduct HITRUST assessments

Incident Response

- Crisis managers – strategize, manage, and defend when privacy and data security issues arise
- Conduct privileged internal root cause investigations
- Interface with state and federal law enforcement
- Direct forensic investigations
- Coordinate with internal communications and PR firms
- Guide through cyber insurance process
- Analyze data breach notification obligations and manage logistics vendors globally

Litigation

- Manage risk to decrease litigation exposure
- Advise and manage preservation and collection of relevant data
- Analyze exposure and develop litigation strategy
- Analyze third-party liability and indemnification issues
- Offer strategic guidance on potential resolution and settlement

Regulatory

- Manage regulatory and third party notifications
- Manage inquiries, investigations, and enforcement actions by state and federal authorities, including state AGs, FTC, CFPB, SEC, DOJ, DFS, OCR
- Prepare and guide clients through Congressional inquiries, investigations and hearings
- Negotiate resolutions

INDUSTRIES

- Education
- Energy
- Financial Services
- Financial Technology (Fintech)
- Forestry and Paper
- Government
- Healthcare
- Hospitality
- Insurance
- Life Sciences
- Manufacturing
- Private Equity
- Professional Services
- Retail
- Sports
- Technology
- Transportation

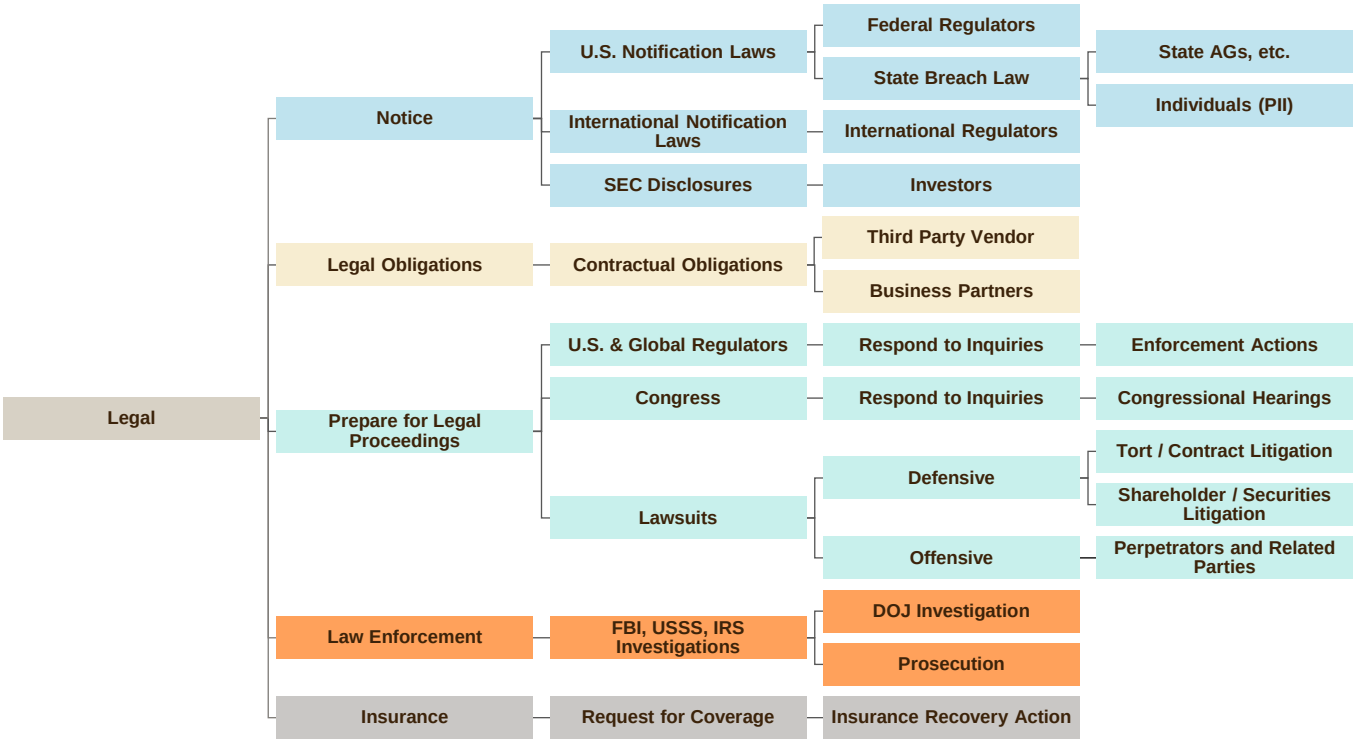
RECOGNITIONS

- *Law360* "Privacy Practice Group of the Year"
- *Law360* "Privacy" and "Cybersecurity" MVPs
- *Cybersecurity Docket* "Top Incident Response 30" award winner

CERTIFICATIONS

- Certified Information Systems Security Professional ("CISSP")
- Certified HITRUST Common Security Framework Practitioner ("CCSFP")
- Certified Ethical Hacker ("CEH")
- Certified Information Privacy Professional ("CIPP")
- Computer Hacking Forensic Investigator ("CHFI")
- Certified Professional in Health Information Management Systems ("CPHIMS")

INCIDENT RESPONSE LEGAL WORKFLOW



King & Spalding has the unique experience of successfully managing all of these legal workflows.

REPRESENTATIVE EXPERIENCE

- **100+ data security incidents** managed in the past several years ranging from phishing, ransomware/malware, skimming, extortion, hacktivists, DDoS attacks, nation-state or national security actions, insider threats, IP theft, and third-party vendor issues
- **60+ nationally recognized attorneys**, including experienced crisis and security response managers, former government lawyers, and trial attorneys with track records of successfully defending data breach investigations and litigation
- Defended multi-district class action litigation brought by consumers, financial institutions, and other businesses arising out of some of the most prominent U.S. data security incidents
- Provide advice proactively on data breach response and handle breach notifications in **all 50 U.S. states and across five continents**
- Thought leader in governance, compliance, and defense, including resolutions
- Vast experience defending government investigations and litigation brought by a variety of regulators, including multi-state consortiums of attorneys general and other state and federal regulators

FOR MORE INFORMATION, CONTACT:

Phyllis Sumner
Partner, Chief Privacy Officer, and Data, Privacy and Security Practice Group Leader
+1 404 572 4799
psumner@kslaw.com

To view or contact our team, please visit kslaw.com.