KRIEG DEVAULT

Data Privacy and Cybersecurity

Krieg DeVault stands ready to assist its clients in cybersecurity and information security risk assessment, data protection and loss prevention, state and federal legal compliance, data breach response, and defense of legal actions associated with data breaches. Cybersecurity depends on corporate governance that understands today's cyber risks. We can guide you through the assessment processes now being recognized as best practices by several federal agencies. For publicly traded companies, we can provide assistance with required SEC disclosures and reporting related to cyber risks and losses. We can also review and analyze cybersecurity insurance products, and resolve insurance policy claims after a cyber-attack. Our attorneys are skilled in handling corporate, litigation, regulatory compliance, intellectual property, and capital financing matters. We provide these services to clients in the financial services, insurance, health care, retail, and other frequently targeted industries. Our deep expertise enables us to effectively and efficiently address almost any matter or claim related to data privacy or cybersecurity.

Focus Areas

Artificial Intelligence (AI)

Risk and Exposure Assessments

- Analyze current practices, policies and procedures related to cyber security
- Update current practices to recognize today's best practices
- Identify current legal vulnerabilities and potential protections
- Identify third party vendors who can help limit risk and loss
- Analyze and report risks, exposures and remedies to executives and directors

Data Protection and Loss Prevention

- Identify critical intellectual property, trades secrets and other assets
- Recommend processes and measures to protect key assets
- Draft policies, procedures and response plans to protect data and limit losses

Compliance

- Counseling related to compliance with state laws and regulations on data privacy and protection
- Counseling related to compliance with federal laws and regulations, including FTC regulations and rulings, on data privacy and protection
- Counseling related to compliance with special provisions of federal law affecting particular industries, such as HIPAA rules and banking regulations

- Counseling related to records retention policies and applicable state and federal legal requirements
- Counseling related to cyber security standards and practices, such as those set by the National Institute on Standards and Technology (NIST) and the International Organization for Standardization (ISO)
- Identification, analysis and description of preventive actions, threats, risks, potential consequences, insurance coverages and other cyber issues related to SEC requirements

Data Breach Response

- Responding to regulatory or criminal investigations related to data breaches
- Reporting cyber security breaches to federal and state authorities, including the filing of criminal reports where necessary and advisable
- Working with forensic investigators to preserve legal privileges, rights and evidence associated with data breach incidents
- Counseling regarding required notifications, investigations, and remedial measures

Defense of Data Breach and Regulatory Compliance Actions

- Breach of fiduciary duty claims
- False advertising and deceptive practice claims
- Breach of state laws and rules on consumer protection, data protection and privacy
- Breach of federal laws and rules on consumer protection, data protection and privacy
- Class action claims

Insurance

- Review of insurance policies and programs for adequacy of coverage regarding potential liabilities, business interruption, breach response costs, fines and penalties
- Review of insurance policy provisions related to specific occurrences, such as lost or stolen laptops, flash drives, or cloud data
- Identifying, negotiating and resolving coverage claims with insurers
- Working with insurance companies to provide their insureds with defenses to data breach actions