GOLDBERG SEGALLA

PRACTICE GROUP CHAIRS

John F. Stephens
Direct — 213.415.7201
jstephens@goldbergsegalla.com

www.GoldbergSegalla.com

CYBERSECURITY AND DATA PRIVACY

Data is everywhere and everything. It is a resource and a currency; it is a lock and a key; it makes up environments and identities. Businesses in every industry recognize data as an endless stream of opportunity. Too often, they fail to recognize the risk.

The Goldberg Segalla Cybersecurity and Data Privacy Practice Group is a multidisciplinary team of attorneys working across the country to counsel, train, and defend clients in numerous industries facing all conceivable cybersecurity and data-related matters. With verdict-tested trial lawyers, preeminent intellectual property litigators, and leading regulatory attorneys collaborating to provide 360-degree cyber counsel, our team helps industry-leading companies, their executives and IT professionals, and their insurers to:

- **Assess** and **address** data security risks
- **Prepare** for cyberattacks and data breaches
- **Create** policies and procedures to mitigate risk and minimize liability
- **Respond** quickly and comprehensively to data security incidents
- **Defend** against post-breach claims and legal proceedings, as well as legal challenges to data-related business practices
- **Navigate** regulatory, statutory, and contractual requirements at every level
- **Anticipate** the future flashpoints that will define the fields of cybersecurity, data privacy, and intellectual property

Data Breach Prevention, Management, and Litigation

Because businesses collect and employ data at every level, technological vulnerabilities, outdated practices and policies, and human errors create risks at every level. Some of these risks include:

- Loss of personally identifiable information — from customers and employees
- Theft of business and trade secrets and other intellectual property
- Attacks on networks and operating systems and resulting business disruption
- Challenges to business practices involving collection and usage of information about customers and the disclosure of those practices
- Exposures stemming from service providers, business partners, and employees

As many companies have learned through experience, the task of managing cyber threats does not begin — or end — with the initial response to a data breach. The company that *reacts* to a cybersecurity incident is positioned for loss, liability, and business disruption. Our approach, by contrast, is comprehensive: By providing counseling and training on how to anticipate risks, prepare for breaches, and execute response plans, we've been able to help our clients avoid serious incidents, limit liability, and implement the best workplace cybersecurity policies and practices.

When attacks or breaches do occur, we help clients respond and recover more quickly and efficiently. Our attorneys are ready to spring into action at a moment's notice to oversee or assist a client's internal incident response team. In addition, clients can rely on our deep bench of accomplished trial lawyers, equipped with experience defending high-profile consumer class actions and multidistrict litigation, to defend any claims that might arise in the aftermath of an attack or breach.

Preparation

Our approach to data breach preparedness and cybersecurity practices is comprehensive, proactive, and adaptable to the global industries and markets in which our clients do business. More importantly, we tailor that approach to fit each client's size and structure, IT resources, business philosophies and practices, and unique risks and vulnerabilities.

ASSESSING RISKS AND LIMITING LIABILITY

Our services often begin with a comprehensive technology liability audit. Our experienced attorneys will identify risks at every level, translating complex legal, technology, security, and information governance issues into plain English and offer practical advice on eliminating, limiting, or mitigating those risks.

We help businesses of all sizes and structures develop policies and procedures to maximize their security and minimize the potential for a data breach. We also help businesses take steps to limit potential liability related to a hacking attack or virus, a data security breach, cybercrime, or other data-related incident.

DATA COLLECTION AND PRIVACY PRACTICES AND REGULATORY COMPLIANCE

Our attorneys are deeply versed in the latest regulatory compliance requirements covering data security, breach preparedness and response, and privacy, and we closely watch the judicial decisions and communications from administrative bodies at every level that indicate how the regulatory landscape is shifting.

We frequently conduct regulatory compliance audits, covering state, federal, and international requirements. We advise companies on requirements pertaining to the collection, storage, and destruction of personally identifiable information, and help realign noncompliant policies or practices.

Our regulatory experience covers:

- Federal and state privacy-related laws and regulations, including:
    - Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH)
    - Children's Online Privacy Protection Act (COPPA)
    - Federal Information Security Management Act (FISMA)
    - Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act)
    - Fair and Accurate Credit Transaction Act (FACTA)
    - Telephone Consumer Protection Act (TCPA)
    - Controlling the Assault of Non-Solicited Pornography And Marketing Act (CAN-SPAM)
    - California's Shine the Light Law, Online Privacy Protection Act, and Confidentiality of Medical Information Law
- State-specific data security and breach response laws
- Federal agency cybersecurity guidelines, including those issued by the FTC, FDA, FCC, and the NIST cybersecurity framework

- International data protection laws, including EU and Latin American requirements

In addition, we leverage our knowledge and experience to assist clients with more complex and industry-specific regulatory requirements, including:

- Compliance with Payment Card Industry Data Security Standards (PCI-DSS) pre-incident and post-data breach obligations
- Conducting due diligence and advising on compliance with privacy and data security laws in the sale and acquisition of company assets, including customer lists and databases containing personally identifiable information
- Auditing multitiered contractual privacy obligations pertaining to third-party online ad-serving companies and instituting policies and procedures for data collection, use, and disclosure
- Advising large multinational retailers on privacy policies, terms of use, and terms of sales to comply with FTC and FCC regulations, and advising on compliance for sweepstakes, advertising promotions, and product-placement agreements

SECURITY POLICIES AND CONTRACTS

We help businesses develop internal, client-facing, and third-party privacy and security policies.

We counsel management on workplace privacy issues, including employee monitoring, whistleblower laws, safeguarding of employee's personal data, Fair Credit Reporting Act requirements in employee screening and investigations, and faithless servant data theft litigation

We also draft consumer-facing disclosures, including privacy policies, terms of use and service, and social media policies

In addition, our team can assist with contracts, agreements, indemnification clauses, and other vehicles to protect against liability. We develop and negotiate security agreements to ensure vendors defend and indemnify our clients on privacy and security issues, and we have experience with agreements involving cloud service providers, co-location facilities, outsourced services, and other entities.

DATA BREACH PROTOCOLS AND CRISIS COACHING

We work with management, IT professionals, and in-house counsel to help our clients develop and train computer security incident response teams (CSIRTs). This includes conducting tabletop exercises and war games and teaching CSIRTs how to administer broader incident response training programs for other employees.

With our cutting-edge crisis coaching, our clients are prepared to act quickly and decisively, preserving digital evidence, meeting changing and immensely complex notification requirements, and managing public relations to minimize reputational harm and help restore confidence in the company.

Response

Committed to providing clients with dynamic, adaptable, and cost-efficient legal service, we are equally capable of working as an auxiliary to a client's CSIRT and in-house counsel or taking the lead and managing every aspect of the response. This is why scores of clients of all sizes and across industries

make Goldberg Segalla their first call after discovering a cybersecurity incident.

BREACH RESPONSE AND CRISIS MANAGEMENT

As trial lawyers, we understand that every decision made before an incident and during a data breach response — from the first call through closing the incident — can dramatically impact potential liability and the course of future litigation. Our comprehensive cyber crisis management services include:

- Coordination of the forensic investigation
- Evidence preservation
- Working with law enforcement
- Advising on multi-state notification requirements
- Advising on HIPAA notification requirements
- Responding to Office for Civil Rights (OCR) investigations and other regulatory and administrative inquiries

POST-BREACH REGULATORY COMPLIANCE

In addition to compliance with regulations pertaining to general data collection and privacy, we also guide clients through the intensely complicated regulatory demands triggered when a breach occurs. These include:

- Federal Trade Commission's Children's Online Privacy Protection Act (COPPA)
- Gramm-Leach-Bliley and Dodd-Frank Acts
- Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act
- New European Union data protection laws
- Disclosure guidelines imposed and enforced by the Securities and Exchange Commission (SEC) as well as multiple state and international insurance industry regulatory authorities

POLICY REASSESSMENT AND PUBLIC RELATIONS

It is impossible to predict and prevent every breach. Sony, the Democratic National Committee, Experian, Ukranian power authorities, and too many others to count offer ample evidence. However, businesses and institutions that respond well to breaches can emerge even stronger after the recovery.

Our post-breach services include working with management, public relations teams, and outside consultants to develop and execute a media and public relations plan that minimizes reputational harm and restores confidence in the company while maintaining compliance with applicable regulatory requirements.

We also help clients seize on the post-breach opportunity to strengthen data protections, running comprehensive post-breach cybersecurity audits and recommending changes to policies, procedures, and response plans as needed.

Defense

Even the strongest and most effective response to a cybersecurity incident leaves open the possibility of costly lawsuits. While companies can take significant steps to limit liability and cut off avenues of plaintiffs' attacks, they may still need the representation of a proven trial team with deep experience in the evolving legal issues unique to cybersecurity and data protection.

BREACH-RELATED LITIGATION

As a firm founded by trial lawyers, we bring to each matter the savvy and successful track record of our Business and Commercial, Product Liability, Professional Liability, Global Insurance Services, and other litigation teams. We also bring extensive experience litigating other matters involving technology, including both prosecuting and defending business-to-business litigation involving website use, data transfer, and data storage issues.

CLASS ACTION DEFENSE

Our Class Action Litigation Practice Group has successfully defended *Fortune* 500 companies as lead counsel in national and state-wide class actions, including high-risk, multimillion-dollar litigation.

A sampling of our trial and litigation experience includes:

- Representing a telephone company in actions challenging the company's use of fax communications as violative of the Junk Fax Prevention Act
- Representing a health care company against a class action lawsuit alleging a data breach of personal health information
- Representing numerous retailers, hospitality and other clients in putative class action lawsuits brought pursuant to the Telephone Consumer Protection Act
- Representing a cellular telephone company in individual and putative class actions challenging the company's debt collection practices under the Telephone Consumer Protection Act

Cyber Risk Insurance Coverage Services

Drawing on the combined experience of our Cybersecurity and Data Privacy Practice Group as well as our Global Insurance Services Practice Group — a renowned insurance and reinsurance practice ranked by market leaders and top global publications as one of the world's biggest and best practices serving this market — we have helped leading insurers and reinsurers anticipate and adapt to emerging risks and meet the growing need for new products. We also assist with reevaluating existing products and pricing models.

Our Cyber Risk Coverage group is prepared to assist insurers and reinsurers with:

- Policy wordings and negotiations
- Underwriting guidelines and coverage counsel
- Reputational risk coverage
- Coverage dispute defense