Data breach lawsuits are highly public. Not a day goes by where a company, large or small, is not dealing with some level of privacy concern or public relations challenge that could be - or already is - a data breach. News headlines, and newly enacted regulations and statutes, show a clear and continuing trend, and individuals and regulators alike insist on the protection of personal, health, financial and identity information.

In these ways, legal exposure has been exponentially-broadened for every business and organization. Businesses must develop processes and safeguards to improve data security and mitigate exposure for damages.

Our business and litigation attorneys defend businesses in high stakes situations, from class action lawsuits grounded in alleged violations of federal, state and local statutes, to claims of breach within the healthcare industry, or alleged failure to comply with HIPAA and HITECH - to everything in-between. The group is led by a certified privacy professional (CIPP-US) recognized as a Privacy Law Specialist by the American Bar Association, a healthcare regulatory authority and a veteran class action litigator.

Our extensive litigation experience makes our team keenly aware of how to best team with our clients to prepare for potential privacy intrusions and data breaches. We craft data maintenance policies and data breach response plans so clients are equipped to respond appropriately in the event of unauthorized access to sensitive data.

We audit existing procedures and practices consistent with industry standards and legal requirements to reduce the risk of a data breach and counsel clients on compliance considerations involving consumer protection regulations, data privacy practices, notification requirements and advertising compliance. Further, our team will coordinate the incident response plan or data breach plan, which includes a team of forensic, security, public relations and insurance professionals.

We are ready to protect our clients against all types of data related litigation, including class actions based on the unauthorized release. Our experience is unparalleled in defending class actions.
EXPERIENCE

- Data incident response to a disclosure of protected health information maintained by a vendor for multiple HIPAA covered entities. This work included full investigation of the matter to determine the extent of the breach and the types of information exposed. From there, the disclosed records were reviewed and analyzed to ensure the company met its reporting and notification requirements under the various federal and state laws applicable to the personal and health information.

- Data incident response to a web server that inadvertently exposed social security numbers and payroll information to the public via Internet search engines. This work involved investigation of the matter to determine the extent of the breach and analysis of all applicable state and federal laws to determine notification and reporting obligations for the company.

- Data incident response plan for a small company, whose hardware was stolen and which hardware allowed access to centralized databases which contained encrypted PII. This work involved investigation into the Personal Information Protection Act of certain Midwestern states to confirm whether notification of the potential breach was required and reporting obligations and best practices, moving forward, for the company.

- Data incident response plan for a small company, whose customers’ accounts were accessed by persons located overseas. This work involved the following: forensic examination, with licensed analysts, into the breach; assessment of the scope of the breach; investigation into the Personal Information Protection Act of certain Midwestern states to confirm notification of the potential breach was required; working with the client and public relations specialists on notice; notifying federal officials; and, crafting a response plan and best practices, moving forward, for the company.

- Data incident investigation of a matter where a company discovered that some of its mailings inadvertently disclosed customer social security numbers that could be viewed in the address window of the envelopes it mailed. This work involved full investigation of the matter to determine the number of individuals who may have been affected by the breach, the types of information involved, and a review of applicable state and federal laws to determine notification and reporting requirements.

- Revision and implementation of a record retention program for multi-state nursing, rehabilitation, and retirement facility. This work consisted of creating a record retention program for multiple facilities across twelve states. The facilities operated by the company maintained different types of electronic medical records and were subject to different state laws, and therefore, our team developed a record retention program that applied to all facilities, across all states.

- Drafting, reviewing, and revising numerous HIPAA Business Associate Agreements on behalf of covered entities, business associates, and sub-business associates

- Obtained ruling from the Seventh Circuit affirming dismissal of a lawsuit against a national testing agency in which plaintiffs alleged claims on behalf of a putative class of 16 million persons that their personal identifiable information had been sold without authorization

- Retained to defend hospital from class action arising from data breach involving protected personal information
Data Privacy, Security & Litigation

- Retained to represent business in class action for alleged violations of Illinois Biometric Information Privacy Act
- Obtained judgment and defeated class certification in FACTA class action lawsuit. The court held that although the plaintiff was personally liable under the cardholder agreement, the entity cardholder was the “consumer”; therefore, there was no private right of action for purposes of the business transaction alleged in the complaint