OUR PRACTICE

Data Incident Response

When incidents arise, Baker Donelson's credentialed data incident response team provides real-time legal and highly technical advice 24/7/365. We assist clients through all phases of a data incident. Our established relationships with forensic investigators, consumer notification mail houses, call centers and public relations firms provide clients the ability to staff even the largest breach matters from the first call. Baker Donelson has been recognized as an authorized NetDiligence Breach Coach® signifying it as a top tier law firm for Data Security, Privacy and Incident Response.

More than one-third of our Data Incident Response Team includes members who are certified by the International Association of Privacy Professionals (IAPP) as Certified Information Privacy Professionals (CIPP/US, CIPP/E, CIPP/A and/or CIPP/C) and two attorneys who are Certified Information Privacy Managers (CIPM). In addition, our team includes a member certified in the Law of Data Security and Investigations (GLEG), a Fellow of Information Privacy (FIP), a Privacy Law Specialist (PLS) and another who is certified as a Payment Card Industry Professional (PCIP).We have attorneys who specialize in handling incident responses in highly regulated industries, such as education, financial institutions and health care.

We assist clients through all phases of a data incident including:

- Working with industry experts to assist with detection, containment and recovery;
- Collaborating with expert third-party ransomware responders to advise clients on ransomware negotiations;
- Coordinating e-Discovery efforts when intrusions are identified;
- Communicating on behalf of our clients with state and federal law enforcement agencies with whom we have established relationships;
- Assisting with assessment and drafting of any state and federal notification obligations;
- Managing communications with vendors, employees, customers and other stakeholders;
- Responding to any state and federal government investigations that result from an incident;.
- Providing analysis to assist in developing post-incident remediation; and
- Representing clients in ensuing litigation, including class action cases, involving data incident issues.

Representative Matters

- Led an incident response team for a medical information technology company after a ransomware incident. Oversaw HIPAA issues, regulator issues and breach notification in multiple states, and managed law enforcement interaction, overseeing crisis communications and litigation arising from the data breach.
- Managed a ransomware incident for a national transportation and logistics company. Led the incident response team in managing breach notification in multiple states, law enforcement interaction, overseeing crisis communications, and compliance with relevant breach notification laws in 30 states.
- Represented a U.S. distribution company for an international lubricants company in managing phishing incident that led to significant wire fraud. Managed the response in dealing with U.S. privacy laws, GDPR, law enforcement interaction and breach notification in more than 14 states.
- Represented a national bank whose vendor experienced a data incident that impacted hundreds of the bank’s corporate customers and more than 250,000 individuals.
- Successfully negotiated a ransomware incident on behalf of a school board in a ransomware attack that resulted in network interruptions to schools providing education to more than 5,000 children.

- Advised a leading e-commerce company that was severely impacted by a phishing attack on multiple employee e-mail accounts that required assessment of regulatory issues under the Payment Card Industry Data Security Standards (PCI-DSS) and responding to regulatory investigations by state attorneys general.
- Successfully represented a large hospital system that experienced a data breach in the subsequent investigation by the Office for Civil Rights.
- Advised a national brokerage firm with respect to potential individual and regulatory notification obligations arising from employee theft of electronic information.
- Represented a bank in a wire fraud incident which resulted in a return of a portion of the stolen funds.
- Assisted a mental health facility in responding to an incident involving a former employee's theft and misappropriation of patient mental health records.
- Advised a network of automotive dealerships on breach notification obligations and remediation of a data incident related to theft of employee information.
- Successfully resolved class action litigation against a national company resulting from data incident relating to a phishing attack on a company employee.
- Assisted a national mortgage company with notification to individuals as well as state and federal regulators in response to an inadvertent email incident.
- Represented a client who was a business associate with their response to an Office for Civil Rights (OCR) investigation regarding an alleged data breach that potentially impacted 3.5 million individuals. We assisted the client with documenting their security protocols and responding to the OCR investigation. The OCR dismissed the investigation with no adverse action.