



Data Breach Response

Data Breach
Response

STRADLEY
SR
RONON

Our Practice

Data security is of paramount importance in the modern age. Customers, industry standards, laws, regulations and good business practice demand that today's companies guard data like never before. And even with state-of-the-art protections and protocols in place, human error and evolving technology leave secure systems vulnerable to attack.

What happens when a data breach occurs? What should be done to assess the breach, mitigate potential damages and comply with laws?

Questions like these strike fear into the hearts of businesses and nonprofits today — and for good reason. An organization that has suffered a data breach could be facing a number of serious consequences — from data leakage or deletion, reporting obligations, regulatory fines or penalties, and lawsuits to reputational harm and loss of critical business-sensitive data.



Our Philosophy

Stradley Ronon's dedicated data breach response team understands the importance of a prompt and proper data breach investigation and response. We and our technology partners help our clients take the quick and prudent actions necessary in the hours, days and weeks following a data breach or incident to understand the scope of the compromise; evaluate the parameters

and elements of unauthorized access, movement or exfiltration of data; and assess the actions needed to maintain legal compliance and mitigate damages. We work with highly trained technology specialists and carefully selected vendors to spearhead the investigation into the breach. Our attorneys recognize that there is no standard approach for a data breach response because there is no standard data breach. Information technology

REPRESENTATIVE MATTERS.

Our data breach response attorneys have handled a wide range of transactions, including:

Represented a **national alumni association of Division I university** to assess and respond to data breach incident, including investigation of breach and notification to state regulators and affected individuals.

Represented a **multistate oncology group** to assess and respond to multiple data breach incidents and prepare HIPAA-mandated breach notifications.

Represented a **religious institution** in monitoring of breach response and undertaking of negotiation/resolution of fines and penalties imposed by United States Office of Civil Rights in connection with privacy breach.

Represented a **regional health care system** in reporting and monitoring of data incident response.

Represented a **health plan** in responding to large-scale vendor breaches, and advised the health plan on the vendors' regulatory and contractual obligations to report the breach.

Assisted a **financial services organization** with evaluation of cyber risk and appropriate policy coverages.

systems vary from business to business, the geneses of breaches vary widely (from criminal hacking or data theft to equipment failure or human error), and legal requirements arising from a data compromise vary from state to state, industry to industry and breach to breach, often depending on the types of information compromised.

Once a breach investigation is underway, where a breach triggers regulatory disclosures and possible fines or penalties, Stradley's attorneys interface with state and federal regulators to ensure legal compliance and minimize damages. We are experienced in regulatory affairs, legal compliance and resolution of regulatory disputes across many industries, including health care, insurance, financial services and education. Where a breach spurs lawsuits, our experienced litigation attorneys are ready to defend our clients against all claims, both serious and spurious, that may be asserted. We work to protect our clients' corporate reputation at every stage in the breach response. If someone else caused the breach, we have significant experience representing clients as individuals or class action plaintiffs.

We also provide comprehensive pre-breach counseling. Our attorneys have extensive experience with the state and federal laws governing the protection of confidential, personally identifiable information; personal health information; and other private records — and what steps are required in the event of unauthorized access. We use this knowledge to help clients assess, prioritize and address their current risks; create and implement best-in-market policies and procedures; develop incident response plans; create training programs and conduct training; assess cyber insurance policies; and review and negotiate vendor agreements to ensure compliance.

The Services We Provide

- **Pre-breach counseling**
 - Assess and mitigate risk
 - Develop policies and procedures
 - Create training programs
 - Review vendor agreements
 - Evaluate cyber insurance policies
- **Post-breach response**
 - Prompt and proper breach investigation with best-in-class technology partners
 - Assessment of data compromise and attendant legal obligations
 - Mitigation of damages
 - Fulfillment of regulatory and disclosure obligations
- **Post-breach litigation**
 - Defense of class action and individual claims
 - Mitigation of damages
 - Resolution of claims through summary disposition, negotiation and/or trial
 - Pursuit of recovery against parties responsible for breach, where appropriate

The Stradley Difference

Stradley brings industry-specific knowledge and regulatory experience to our data breach response engagements. Also, in conjunction with our robust government affairs practice group, we stay on the cutting edge of legal developments regarding data breaches, and help



shape the laws and legal obligations in this field. Our attorneys have in-depth regulatory experience in industries including financial services, health care, higher education, manufacturing, insurance and many others particularly prone to data breaches. Our attorneys regularly speak, write and train others on data security issues, and we use this knowledge to keep our clients in compliance, prepared to respond if and when a breach occurs and, with the comfort of Stradley as a trusted adviser, focused on their business. To assist our clients with bolstering their compliance and risk mitigation practices, one of our attorneys is an IAPP Certified Information Privacy Professional and can provide advice to clients regarding U.S. privacy and data protection laws, compliance with those laws and risk mitigation practices.

For more information on our data breach response practice, visit
www.stradley.com/data-breach.



CONTACT

Jeffrey D. Grossman
215.564.8061
jgrossman@stradley.com

ABOUT STRADLEY RONON

For more than 95 years, Stradley Ronon has helped private and public companies – from small businesses to Fortune 500 corporations – achieve their goals. With eight offices and more than 200 attorneys, Stradley Ronon is proud to help companies manage their legal challenges and grow their businesses.

www.stradley.com

LOCATIONS

Pennsylvania
Washington, D.C.
New York
New Jersey
Illinois
Delaware



This communication is provided as a general informational service to clients and friends of Stradley Ronon Stevens & Young, LLP. It should not be construed as, and does not constitute, legal advice on any specific matter, nor does this message create an attorney-client relationship. The enclosed materials may have been abridged from other sources. They are provided for educational and informational purposes for the use of clients and others who may be interested in the subject matter. This material may be considered attorney advertising in some states. Please note that the prior results discussed in the material do not guarantee similar outcomes.

© 2023 Stradley Ronon Stevens & Young, LLP