SEYFARTH SHAW

Global Privacy & Security Team

Incident Management

We recognize that the unauthorized disclosure or use of information is a fact of life, and needs to be responded to seriously and quickly. We employ our rapid response Global Privacy & Security (GPS) Team to investigate such incidents and assess our client's responsibilities under applicable laws and contracts.

Our incident management experience includes conducting internal investigations, monitoring vendor investigations, drafting required notices to regulators, individuals and the media under state and federal laws, responding to regulators and consumer inquiries, submitting takedown requests to social media sites, consultation on mitigation activities, and security breach incident response.

Incident Response Planning. While our main objective is to help our clients avoid a privacy or security breach altogether, Seyfarth's GPS Team works with clients to develop contingency plans for data breach incidents. In the event of an actual breach related to personal information, we advise our clients on how they can best communicate with law enforcement, regulators, employees, consumers, and consumer reporting agencies.

Security Breach Management. Among the areas where we have particular knowledge is security breaches. We have handled literally hundreds of incident response situations, from conducting formal investigations following a breach, to negotiating indemnifications and responsibilities for an incident, to managing reporting for breaches. We also have assisted in negotiating with forensics companies, service providers, regulators, attorneys general and PR firms regarding the handling of a security incident.

Our Capabilities:

- ☑ Development of contingency plans for data breach incidents
- ☑ Counseling regarding risk management and insurance coverage
- ☑ Response protocols and mitigation
- ☑ Internal investigations
- ☑ HIPAA security incident and breach investigations
- ☑ HIPAA audit and HHS inquiry responses
- ☑ Reporting obligations
- ☑ Social media public defamation or brand disparagement
- ☑ Employee terminations

Track Record of Results

- Counseled a hotel franchisee with respect to a security breach involving its Point of Service (POS) systems that affected over 3,000 individuals throughout the country. Our team supervised the review of forensic experts analyzing the root causes, negotiated with privacy counsel for the franchisors, made determinations concerning notifications to be sent as well as prepared, edited and/or negotiated the terms of the notifications to consumers and regulators, and managed responses to the media and regulators.

- Counseled an insurance brokerage firm in investigating and responding to security incidents, the largest of which affected more than 380,000 individuals throughout the U.S. Seyfarth coordinated investigating the incident, reconstituting information, developing notification strategy, and notifications and discussions with affected clients, service providers and regulators. We have served as outside privacy counsel for this client for 10 years, handling domestic and international privacy matters, Gramm-Leach-Bliley, HIPAA and Massachusetts database security compliance in addition to security breach matters.

- Counseled a client with respect to a HIPAA privacy breach whereby protected health information was erroneously distributed by a third-party administrator. Seyfarth advised the client with regard to mitigating the damage and documenting the breach in an investigative report, as well as represented the company with regard to the third-party administrator's breach of the business associate agreement. The incident resulted in an employee filing a privacy complaint with Health and Human Services/Office of Civil Rights, which the client was able to close with no penalties upon production of the investigation report and other documentation prepared by Seyfarth.

- Counseled Fortune-ranked construction management and petroleum refinery clients regarding a potential security breach involving stolen personal information by an employee of a service provider. Seyfarth provided analysis under both HIPAA and state database security breach laws and negotiated with service provider counsel regarding indemnification and credit monitoring (both of which were resolved in our clients' favor).

- Conducted an extensive investigation, HIPAA risk analysis and state database security breach analysis involving a short-term computer system vulnerability that was not exploited and ultimately determined not to be a breach under applicable laws. Since the vulnerability related to approximately 150,000 health plan participants, it was extremely important that the analysis be extensive and accurate. This required interviewing employees with the client and the vendor, verification of all of the relevant facts and an extensive legal analysis in order to reach a conclusion.

SEYFARTH SHAW

www.seyfarth.com