What to Do When You Find Yourself in the Data Breach Club

By Veronica Jackson, Miles & Stockbridge

More and more companies are likely wondering what they should do in the event that they are faced with a data breach that exposes the personal data of their employees or customers. Data security incidents involve complex legal issues that must be navigated carefully to reduce the risk of improper (or unnecessary) breach notification, attention from state and federal regulators, and potential class actions related to the exposure of personal information. There are several key steps a company should take upon discovery of a data breach. While these steps are numbered, many of them must happen both immediately and simultaneously.

First, immediately contact your company's incident response team pursuant to your Written Information Security Plan (or "WISP"). Second, contact law enforcement and any relevant insurance carriers to assist with coverage of costs for the data breach response effort and to prevent waiver of potential coverage for tardy notice. Third, quickly assess the scope of the breach (i.e., whether the breach is ongoing, whether data was acquired or simply accessed by the hacker, who suffered a breach of their personal information, what type of information was exposed, and the likelihood that the affected persons will suffer harm as a result of the breach). Fourth, stop the breach, if possible, through remedial data security measures, possibly with the assistance of a forensic IT consultant to bolster your company's security systems. Organizations that have already suffered from a breach especially must consider what additional safeguards (including employee training) should be implemented to avoid another breach in the future. Fifth, analyze data breach compliance requirements by identifying the jurisdictions of residence for the affected population and assessing what notification requirements are triggered by each applicable statute.

Data breach compliance requirements also may be triggered by the regulatory framework covering the type of information that was exposed (*i.e.*, HI-TECH and HIPAA compliance for personal health information). For affected persons residing in Maryland, for example, notification is not required if, after the requisite investigation, the business determines that personal information has not been or is not likely to be misused. (Documentation of that conclusion, however, must be retained by the entity for three years.) In instances where notification is required, even for just one Maryland resident, notice must first be sent to the Maryland Attorney General's data breach notification department. Maryland also recently amended its notification statute to, among other changes, require that companies make any requisite notices within forty-five days from when the company determines that notice is required. In the District of Columbia, on the other hand, there is no "likely harm" exception to the notification requirement and notice to the Attorney General is not required. In instances where 1,000 or more residents are receiving notice at a single time, both Maryland and the District of Columbia require that notice be sent to all nationwide consumer reporting agencies regarding the timing, distribution and content of the notices.

Finally, prepare a data breach response plan that attempts to mitigate potential harm to the affected population and complies with applicable data breach requirement statutes and regulations. Since the Supreme Court's decision in *Spokeo v. Robins* attempted (but failed) to clarify the legal standard for what constitutes sufficient harm to a person affected in a data breach for legal standing purposes, a Circuit split has emerged. Because it remains unclear what level of risk for future harm or actual harm is required (short of actual identity theft), efforts to minimize the risk of identity theft and other subsequent harm, as well as providing free preventative services to affected people, are valuable tools that may provide a defense against subsequent litigation stemming from the data breach. Many organizations elect to provide an affected population with identity theft prevention services that monitor their credit and also aid them in any credit repair efforts they may need should they fall victim to identity theft. State attorneys general also look at whether an organization is providing such services to affected persons and for how long when reviewing data breach response notifications.

Veronica Jackson is a lawyer in the Labor, Employment, Benefits & Immigration Practice Group of Miles & Stockbridge. She is a Certified Information Privacy Professional by the International Association of Privacy Professionals. In the area of data privacy and security, Veronica counsels clients through incident response efforts, privacy law compliance, privacy policies and training.

Disclaimer: This is for general information and is not intended to be and should not be taken as legal advice for any particular matter. It is not intended to and does not create any attorney-client relationship. The opinions expressed and any legal positions asserted in the article are those of the author and do not necessarily reflect the opinions or positions of Miles & Stockbridge, its other lawyers or ACC Baltimore.