BCLP. Client Intelligent

Insights

WHAT ARE THE OBLIGATIONS TO BUSINESS PARTNERS IN THE EVENT OF A DATA BREACH?

Jan 16, 2020

As of January 1, 2020, California became the first state to permit residents whose personal information is exposed in a data breach to seek statutory damages between $100-$750 per incident, even in the absence of any actual harm, with the passage of the California Consumer Privacy Act ("CCPA"). The class actions that follow are not likely to be limited to California residents, but will also include non-California residents pursuing claims under common law theories. A successful defense will depend on the ability of the breached business to establish that it implemented and maintained reasonable security procedures and practices appropriate to the nature of the personal information held. The more prepared a business is to respond to a breach, the better prepared it will be to defend a breach lawsuit. To help our clients prepare for the CCPA, Bryan Cave Leighton Paisner is issuing a series of data security articles to empower organizations to focus on breach readiness.

Contractual Obligations to Business Partners

In situations in which a security incident involves data that is wholly owned by an organization, there may be few, if any, obligations for the organization to notify business partners. Often, however, business partners may have an interest in the information impacted. For example, if an incident involves data of another entity for which your organization is performing services, you may have an obligation in your service agreement or under state data breach notification statutes to notify that entity of an actual (or suspected) security incident. The contractual requirement sometimes requires notifying the partner in a relatively short time frame (*e.g.,* immediately or within 24 hours) when an incident is *suspected*. As another example, if an incident involves payment card information that you received from consumers, the agreement that you have with your payment processor or merchant bank may similarly require that you notify those entities or additional third parties (*e.g.,* Visa, Mastercard, Discover, and American Express) of a potential security incident.

Data breach notification laws typically place the onus on the *owner* of data to notify affected persons when sensitive personal information is wrongfully accessed or acquired. For instance, a data storage vendor may possess a database that contains Social Security numbers, but the database may belong to the vendor's client. In many states, the vendor may not have an obligation

to notify affected persons itself, but it most likely has a legal obligation to notify its client, who in turn will have an obligation to notify the affected persons. Similar rules apply under the GDPR. A data processor is required to notify the data controller in the event of a data breach, and the data controller bears the responsibility for notifying the supervisory authority and the data subjects.

In many instances, although the data owner technically has the legal obligation to notify affected persons, the data owner will look to the data user to make the notification or pay for the costs of notification.

Tip: An organization may wish to prepare a spreadsheet of the data notification provisions included in its key contracts. In the event of a breach, the spreadsheet can be quickly consulted to determine the obligations, as such contracts typically include short timeframes during which notification must occur.

BCLP is working with clients to assess – and mitigate – risks by putting in place the policies, procedures, and protocols needed to address data security breach issues.

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Linda C. Hsu

Los Angeles

linda.hsu@bclplaw.com
+1 310 576 2192

should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.