BCLP. Client Intelligent

Insights

DATA BREACH LITIGATION PREPARATION: WHAT TYPES OF SERVICES SHOULD THE ORGANIZATION OFFER TO CONSUMERS AFFECTED BY A BREACH?

Feb 04, 2020

As of January 1, 2020, California will become 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.

Credit Monitoring and Identity Theft Offerings

A growing number of states, e.g., Connecticut, Delaware, and Massachusetts, require that a company provide ID theft-related services if a breach involves Social Security numbers. Connecticut requires such services be provided for 24 months. Other data breach notification statutes do not require that an organization offer any services to consumers whose information was involved in a breach.

Nonetheless, organizations typically consider whether to voluntarily offer ID theft-related services (*i.e.,* monitoring a consumer's credit report for suspicious activity), identity restoration services (*i.e.,* helping a consumer restore their credit or close fraudulently opened accounts), or identity theft insurance (*i.e.,* defending a consumer if a creditor attempts to collect on a fraudulently opened account and reimbursing a consumer for any lost funds). For those organizations that choose to offer one or more ID theft-related services, they are also faced with the question of how long to offer each of the services; durations typically range from one year to three years. In September 2014, California amended its personal information privacy law to require that businesses that choose to

provide identity theft prevention and mitigation services do so for 12 months at no cost to the affected persons.

There are several factors to consider when choosing what (if any) services to offer consumers. In terms of mitigating potential harm, credit monitoring (and to a lesser extent identity restoration services and identity theft insurance) is focused on the prospect that a third party might open a financial account in a consumer's name. Not all breaches involve data that would permit a third party to open a financial account, however. For example, while a breach that involved a consumer's name and credit card number could theoretically lead to unauthorized charges placed on the credit account, name and credit card number alone are insufficient to attempt to open a new financial account, and unauthorized charges on an existing account are unlikely to be identified by credit monitoring.

Although credit monitoring may not be connected to the risks attendant with many breaches, an organization should consider whether a failure to offer the service – even if unconnected to the breach – could be misunderstood by consumers and regulators as a failure by the company to adequately protect consumers. Conversely, offering such services where the organization views them as unconnected to the risk of harm could be construed in litigation as an admission that the company believes harm is likely to occur.

If your organization chooses to offer credit monitoring, identity restoration services, or ID theft insurance, in-house counsel should carefully consider the vendors that are selected to provide the services and the contractual limitations on those vendors. Specifically, vendors (and, by association, the breached organizations which retained the vendors) have been criticized for the following:

- Requiring consumers to submit sensitive personal information to the vendor in order to enroll in the offered service(s);
- Attempting to "upsell" consumers on additional protection services that are offered by the vendor, but the price of which are not covered by the organization;
- Deceptively advertising or describing the credit monitoring, identity restoration, or ID theft insurance services or products;
- Applying inadequate security to protect the information of consumers who enroll in the credit monitoring, identity restoration, or ID theft insurance products.

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
- California Consumer Privacy Act

MEET THE TEAM

Linda C. Hsu

Los Angeles

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