BCLP. Client Intelligent

Insights

DATA BREACH LITIGATION PREPARATION: SHOULD COMPANIES COMMUNICATE WITH THE PUBLIC/MEDIA AFTER A DATA BREACH?

Jan 21, 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.

Communication to the Public/Media

After a breach occurs, organizations should consider a proactive and reactive public relations and media strategy. A proactive strategy assumes that your organization has control concerning when, and what, information will be conveyed to the public, to the media, and to the impacted consumers about the breach.

State and federal laws may require an organization to notify consumers or the media within a certain time period of discovering a breach. For example, HIPAA requires many organizations in the health care industry to notify prominent media outlets if 500 or more individuals within a geographic area are impacted.

Even if no federal or state law requires an organization to notify the media, there may be significant advantages to notifying individuals as early as is practical. The sooner individuals are notified that sensitive personal information may have been exposed, the sooner they can take proactive steps to reduce the likelihood that they will become the victim of identity theft or other fraud. For example, an early informed consumer can request that the major credit reporting agencies put a freeze on

their credit or change the passwords associated with financial accounts. If proactive measures prevent individuals from becoming victims of fraud, they also reduce the likelihood that the consumer will sue your organization for actual damages allegedly incurred by the breach. Early notification also may reduce the likelihood of allegations by regulators that your organization did not comply in a timely fashion with data breach notification laws.

While early notification can be beneficial in some situations, in other situations, premature notification can harm both consumers and the organization. Data breach investigations, particularly those that involve the exposure of electronic records, can be extremely time-consuming. It may take some time to identify the true scope of the breach to determine whether a breach, in fact, occurred, or to verify which individuals may have been impacted. It also takes time to create an accurate communication to individuals and to coordinate with third parties, such as a mailing house, or ID theft protection service providers.

An organization that notifies consumers before the investigation is complete risks providing inaccurate information concerning the scope and nature of a breach. Specifically, some consumers may be told that their information was exposed when the investigation ultimately reveals that not to be the case. These consumers may be subjected to unnecessary worry, cost, and inconvenience to try to mitigate harm that will never materialize. Conversely, other consumers may be told that their information was not exposed when the investigation ultimately reveals that it was. These consumers may be confused and may fail to take protective measures that would mitigate a heightened risk of identity theft. Clarifying initial inaccurate information provided by an organization can be both difficult and time-consuming and can deflect the organization's resources and attention from responding to the breach itself. In addition, confusion by consumers and efforts to clarify that confusion can significantly increase the risk of litigation, as some consumers may incorrectly believe that the organization provided erroneous information intentionally. Such a belief may adversely impact your brand and reputation.

A public relations firm experienced in handling communications concerning data breaches may serve as a useful resource. Once an organization has decided on its proactive communications strategy, in-house counsel should work closely with the organization's communications resources concerning how that strategy will be implemented. Among other things, the following communications channels should be considered:

- **Traditional Media**. The organization should consider whether to provide information in print media or television media. This may take the form of a crafted press release or direct communications to specific reporters.
- **Social Media.** To the extent that your organization desires to disseminate information quickly, you should consider the potential risks and benefits of utilizing social media.

While it is important to consider the pros and cons of providing information to the public as part of a proactive media strategy, in many situations, an organization does not control when the public becomes aware of a breach. The media may learn about a breach from a business partner, a government agency, a consumer, or a disgruntled employee. You should anticipate that, in such a situation, the media may report inaccurate information or may report speculation as "fact." The following factors should be considered:

- **Difficulty Correcting the Record.** Although a media report may be based on speculation, if the organization's investigation has not concluded, it may be difficult for the organization to correct the record.
- **Difficulty Conveying the Tentative Nature of Early Information.** If the organization makes a statement to the media based on the limited information that is available, there is a strong risk that the media may characterize the statement as the "position" of the organization and not fully explain qualifications and limitations of that position.
- **Developments In Information May Be Interpreted as Intentional Withholding.** As the investigation develops, the media may misinterpret additional information that is provided by the organization. The best case scenario may be that the media characterizes such information as a "revision" by the company. The worst case scenario may be that the media implies that the company should, or could, have disclosed the new information earlier.
- **New Headlines.** Each time an organization releases information to the media, it is a potential opportunity for the media to create a new headline concerning a breach. Establishing a pattern of continuously updating the media may result in creating a constant stream of media attention concerning your organization.

For additional information, BCLP's Data Security Breach Handbook provides a comprehensive guide on how to respond when a breach happens and how to prepare your organization before one occurs. 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.

For more information and resources about the CCPA visit http://www.CCPA-info.com.

RELATED CAPABILITIES

- Data Privacy & Security
- California Consumer Privacy Act

MEET THE TEAM

Linda C. Hsu

Los Angeles

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