BCLP. Client Intelligent

RetailLawBCLP

COUNTDOWN TO THE CCPA: WHAT IS LEGALLY CONSIDERED TO BE A DATA BREACH?

Nov 08, 2019

When the California Consumer Privacy Act ("CCPA") takes effect in January 2020, California will become the first state to permit residents whose personal information is exposed in a data breach to seek statutory damages of between $100-$750 per incident, even in the absence of any actual harm. 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 get ready for the CCPA, Bryan Cave Leighton Paisner is issuing a series of data security articles to empower organizations to focus on breach readiness.

Understanding the Nature and Scope of Data Security Events, Incidents, and Breaches

It has been several years since data breaches first emerged as the lead news story. In 2016, then attorney general Kamala Harris published the California Data Breach Report to provide a comprehensive analysis of reported data breaches from 2012 to 2015. During that four-year time period, nearly 50 million records of Californians had been breached, the majority resulting from security failures. Despite increasing security and technology advancements, companies are still grappling with how to stay ahead of hackers and when they cannot, how to respond to a breach in a way that minimizes business disruption and reputation risk. In order to effectively respond to a data security incident, in-house counsel must understand what a "security incident" entails, what their organization should do to prepare itself before the incident occurs, and what practical considerations will confront the organization when a security incident arises.

What is a "Data Breach"?

People sometimes refer to a "data breach" loosely as any situation in which data may have been removed from, or lost by, an organization. Technically, however, "data breach" is a legally defined term that typically refers in the United States to a subset of such situations where there is evidence of an unauthorized "acquisition" of or "access" to certain types of sensitive personal information (e.g., Social Security numbers, driver's license numbers, or financial account numbers) that trigger a

legal obligation by an organization to investigate the situation and to notify consumers, regulators, or business partners. As a result, it is important to realize that many of the situations that are referred to as "data breaches" in the media, and possibly by others in an organization may not in fact meet the legal definition of the term. For the purpose of clarity, we use three terms to refer to security situations: a data security "event," "incident," and "breach."

1. **Security Events**

A "security event" refers to an attempt to obtain data from an organization or a situation in which data could, theoretically, be exposed. Many security events do not necessarily place the organization's data at significant risk of exposure. Although an event might be serious and turn into an "incident" or a "breach," many events are automatically identified and resolved without requiring any sort of manual intervention or investigation and without the need for legal counsel. For example, a failed log-in that suspends an account, a phishing email that is caught in a spam filter, or an attachment that is screened and quarantined by an antivirus program are all examples of security events that do not lead to an incident or breach and require little to no legal action.

2. **Security Incidents**

"Security incident" refers to an event for which there is a greater likelihood that data has left, or will leave, the organization, but uncertainty remains about whether unauthorized acquisition or access has occurred. For example, if an organization knows that a laptop has been lost, but does not know what information was on the laptop or whether it has fallen into the hands of someone who might have an interest in misusing data, the situation is a security incident. Another way to think of a security incident is as a situation in which you believe that electronic data that contains personal information may have been improperly accessed or acquired. Security incidents almost always necessitate that an entity conduct a thorough investigation to test the suspicion that personal information was improperly accessed or acquired. Put differently, companies conduct investigations to determine whether there is, or is not, evidence that would redefine the "incident" as a "breach."

Security incidents are attributable to a variety of different causes—sometimes referred to as "attack vectors." While most breaches are caused by third parties, in 2018 approximately 26.3% were a direct result of employees from within an organization, which includes both inadvertent disclosure (i.e., human error) and insider threats.

3. **Security Breaches**

As discussed above, a data "security breach" is a legally defined term. The definition varies depending on the data breach notification laws that are at issue. As a general matter, a security breach refers to a subset of security incidents where the organization discovers that sensitive information has been accessed or acquired by an unauthorized party and that acquisition has created the possibility that a consumer might be harmed by the disclosure. In the laptop example

provided above, if your organization determines that the laptop was stolen and it contained unencrypted Social Security numbers, the incident would fall under the definition of a "security breach." Security breaches almost always dictate that your organization consider the legal requirements of data breach laws.

For additional information, BCLP's Data Security Breach Handbook (2019 Edition) provides a comprehensive guide on how to respond when a breach happens and how to prepare your organization before one occurs. Click here for the handbook. 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 PRACTICE AREAS

- Retail & Consumer Products

MEET THE TEAM

Linda C. Hsu

Los Angeles

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