BCLP. Client Intelligent

**Insights**

# DATA BREACH LITIGATION PREPARATION: SHOULD COMPANIES CONTACT LAW ENFORCEMENT AFTER A DATA BREACH?

Jan 23, 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 with Law Enforcement

Many security incidents involve a crime that has been committed, or is in the process of being committed, against an organization. For example, when someone attempts to hack into an organization's network to obtain sensitive personal information, they may be committing criminal trespass, theft, attempted identity theft, computer fraud, wiretapping, or economic espionage, among a host of other statutory violations. Accordingly, the organization should consider reporting it to law enforcement. Contacting law enforcement may result in assistance stopping the criminal behavior, useful information that may help the organization's investigation of the incident, or prosecution of the culprit. It also may help demonstrate to the public that the organization was diligent in investigating the incident and taking steps to protect consumers.

Note, however, that law enforcement's resources and ability to assist an organization, particularly when there is no identifiable monetary loss (e.g., actual fraud as a result of breached systems or money lost due to wire transfer fraud), is limited. Thus, it is important to set your incident response team's expectations about the extent to which law enforcement will be helpful.

There is no single federal or state law enforcement agency with jurisdiction over data breaches. In general, however, in-house counsel should consider contacting the Federal Bureau of Investigation's Cybercrimes unit or the United States Secret Service with regard to a security incident that involves the electronic exfiltration of information. The FBI offers online reporting at www.IC3.gov, although often organizations reporting minor security breaches will not receive a response after making an online report. For security incidents that involve paper records or known individuals (*e.g.,* employees or former employees), in-house counsel also might consider contacting municipal law enforcement in the jurisdiction in which the individual resides or works.

When communicating with law enforcement, in-house counsel should be cognizant that information provided to law enforcement may lose the protection of the attorney-client privilege. Recent legislation – including the Cyber Security Act of 2015 – is designed to help companies share information with the government without losing privilege protection, but such legislation should be closely examined, as their applicability typically depends on the type of information shared, how the information will be used, and the law enforcement agency with which it will be shared.

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.

## 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

---