BCLP. Client Intelligent

Insights

DATA BREACH LITIGATION PREPARATION: WHAT SHOULD ORGANIZATIONS CONSIDER WHEN NOTIFYING CONSUMERS OF A DATA BREACH?

Jan 30, 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.

1. How quickly must an organization notify affected consumers of a data breach in the U.S.?

Most of the state statutes do not strictly define the timing in which notification must occur. Only a few states prescribe specific deadlines (*e.g.,* Louisiana (60 days), Wisconsin (45 days), and Florida, Colorado, and Washington[1](30 days)). Generally, the notification must occur in the "most expedient time possible and without unreasonable delay." How this language is interpreted may vary, but as a general rule the organization should endeavor to notify affected consumers within 30-45 days. The triggering point is generally the date on which the organization determined it had a breach or had a reason to believe a breach may have occurred.

All states will permit organizations to delay notification if law enforcement determines that notice to individuals would interfere with a criminal investigation.

Tip: As a practical matter, law enforcement will rarely advise an organization to delay notification. If your organization intends to delay notification based on a request by law enforcement, consider obtaining written confirmation of that request to explain any delay at a later time.

2. What information does the consumer notice have to include?

Many state laws do not provide any instruction or requirements concerning the content of a notification, leaving the content to the discretion of the organization. Other states mandate that some or all of the following information be included in the notification letters: (1) a description of the breach; (2) the approximate date of the breach; (3) the type of personal information obtained; (4) contact information for the credit reporting agencies or government agencies; (5) advice to the consumer to report suspected identity theft to law enforcement and/or a reminder to be vigilant about identity theft; and (6) a toll-free number provided by the reporting organization where consumers can call with questions about the breach. However, because there are many deviations from what the states require, each individual statute should be examined in connection with reporting a breach.

California designates a particular format that should be followed. Generally, in multistate breaches, organizations will opt to use the California format even for residents of other states where it is not required.

Massachusetts' statute contains a significant departure from the other states in that it *prohibits* an organization from identifying the nature of the breach. Thus, in a nationwide breach, in-house counsel should consider whether Massachusetts residents should receive a slightly modified notification letter compared to the one sent to residents of other states. In practice, however, many organizations will opt to use one letter template for all impacted individuals, including Massachusetts' residents. In addition, Massachusetts and Illinois both prohibit companies from providing in the notice the number of those states' residents impacted by the breach.

3. How must an organization notify affected consumers?

The majority of states require that consumers be notified in writing. Email notice can provide substantial costs savings over mailing written notice, but notification through email is only permitted in approximately one-third of the states and in those states there are restrictions on when email notice is permissible. For example, many states require that the consumer either has consented to receive electronic notices, or that the primary method of communicating with the consumer has been through email, such that the consumer would not be surprised by receiving email notification. Additional states permit email notification if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing set forth in 15 U.S.C. § 7001, the federal ESIGN Act.

If your organization is considering an electronic notice, you should evaluate the risk that third parties may attempt to create fake electronic messages that appear to originate from your organization (a practice called "spoofing"). These messages can further victimize consumers by having them provide additional personal information (a practice called "phishing"). For example, instances have been reported where individuals send fake notification letters that ask consumers to

click on a link that, in turn, downloads malware onto the consumer's computer, or to send PII to a service allegedly providing credit monitoring. As a result of these risks, some companies have chosen not to send electronic messages concerning a security breach. Or some companies make clear in the electronic messages they do send that the company will never request that consumers transmit additional PII over email or click on a link to obtain credit monitoring. In other situations, companies have determined that the risk of phishing in their industry is low and have opted (where permitted) to notify consumers by email.

Most states will permit "substitute notification," which is typically some combination of email, posting information about the breach on the organization's website, or notifying the media. However, the circumstances under which such notice is permitted vary widely. Substitute notice generally is permitted only when the notification costs are great or the number of persons to be notified is large; what is considered "large" varies significantly from state to state. For example, Arizona permits substitute notification if the notification cost exceeds $50,000, or the class of persons exceeds 100,000, or if the organization has insufficient contact information for affected consumers. New Jersey (and many other states) will not permit substitute notice unless the cost exceeds $250,000, or the class exceeds 500,000, or if the organization has insufficient contact information for affected consumers.

Many states permit an organization to create its own notification procedures for the treatment of PII if its information security policy complies with the timing requirements under the state law. If notification is done in accordance with the organization's policy, the organization is considered to have complied with the state law.

4. Should an organization ever voluntarily notify consumers of a breach?

In many instances involving a data breach, notice will not be required by any state or federal laws. However, there are many situations in which an organization may choose to voluntarily notify consumers. For example, while a minority of states requires notification for a breach of electronic account user names/email addresses and passwords, if such a breach also involved consumers in other states, the organization may want to notify all affected persons for consistency.

In addition, breaches often become public through other means (*e.g.*, internet blogs, the media). Self-notifying, even when such notification is not legally required, may help the organization frame the message before the message is framed for it by a third party. Although the organization may face initial criticism for its data security practices, consumers may ultimately appreciate an organization's candor in connection with a breach.

5. Is notification required to any other parties?

Various state statutes also require third-party notification. Some states will require the organization to notify the three major credit reporting agencies in the event of a breach involving a minimum number of affected persons (typically, at least 1,000). The statutes with such a requirement

generally do not set forth what information should be provided to the credit reporting agencies other than the timing, distribution, and content of the notices that the organization intends to send to consumers.

In addition, as discussed above, if the organization is not the data "owner," as defined by the various statutes (typically, an organization that maintains or stores, but does not own or license, personal information), then many state statutes will require the organization to notify the data owner of the breach "immediately" or "as soon as possible." Oregon requires data vendors (organizations that process data on another's behalf) to notify the data owner within 10 days of discovering the breach. Once notified, the obligations would then fall to the data owner to comply with the consumer notification requirements of the various statutes. Oregon requires the data vendor to notify the attorney general if the data owner fails to do so.

Many states have a requirement that the state government (usually the Attorney General's office) should be notified of a breach under certain circumstances. Of those states, most require notification in the event of a breach involving any number of persons, while others require that the breach impact a minimum number of residents before state government notification is necessary. For example, New York requires government notification in a breach involving any number, Florida requires government notification when 500 Florida residents are affected, and Arkansas, Hawaii, Missouri, and South Carolina only require state government notification if the breach involves at least 1,000 residents.

For states requiring government notification, the statutes again vary on what information is required to be reported. Most states will require that the reporting organization provide a copy of the consumer breach notification letter, identify the number of residents notified, and the timing of the notification. Some states, e.g., Indiana, North Carolina, and New York, have forms prepared by the state for use in connection with government notice of a breach, and these forms are available online. In the event of a multistate breach, each statute should be carefully examined to ensure full compliance.

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.

---

1. Effective March 1, 2020.

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
