California Legislature to Clarify, Expand Data Breach Notice Requirements

August 18, 2011

A bill that is close to final passage in Sacramento will clarify and slightly expand notification requirements upon a breach of unsecured personal data of California residents, including financial, health or health insurance information. Currently the law requires written or electronic breach notification, but does not mandate any particular content for notifications. Senate Bill 24 will amend California Civil Code § 1798.29 (applicable to state agencies) and § 1798.82 (applicable to private owners or licensors of data) to specify what information must be conveyed in notification of a breach. Specifically, the measure requires that the notification:

- Be written in plain language
- Be dated
- Include contact information regarding the breach, the types of information breached, and the date, estimated date, or date range of the breach
- Include toll-free phone numbers for the major credit reporting agencies
- Describe whether notification was delayed due to law enforcement investigation.

Optional language that may be added to the notice includes information about what the notifying party has done to protect individuals whose information has been breached, and advice on steps affected individuals can take to protect against identity theft or other consequences of the breach.

The new law also slightly expands notice duties, by requiring that an electronic copy of the breach notification be sent to the Attorney General in each instance where a single breach affects more than 500 California residents. Additionally, it requires those making use of "substitute" notification to also notify the Office of Privacy Protection within the State and Consumer Services Agency (state agencies must instead notify the Office of Information Security within the California Technology Agency). Substitute notice may be provided upon demonstrating that the cost of providing notice would exceed $250,000, or where more than 500,000 individuals' data is affected. In addition to the new agency notification duty, substitute notice requires all of the following:

- E-mail notice where valid e-mail addresses are available;
- Conspicuous posting of the notice on the breaching party's web page; and
- Notification to statewide media.

Similar to rules under HIPAA/HITECH, notification is only required if unencrypted data is released, and notice is not required where the data exposure is limited to "good faith acquisition by an employee or agent of the business for purposes of the business." Civil Code § 1798.82(g). Under both federal and state law, however, notice is required not only upon discovery of an actual security breach but also upon formation of a reasonable belief that a breach occurred.

Unlike HIPAA/HITECH, which specify a maximum 60-day notice period, the California law does not specify a notice time period, requiring only that it be provided "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, [. . .] or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Civil Code § 1798.82(a). A business that simply maintains data but does not own or license it must "immediately" provide notice of the breach to the owner or licensee of the data, which in turn will notify the affected individuals.

Finally, there are two "safe harbors" exist in regard to notification:

• Businesses that are “covered entities” under HIPAA need only satisfy HIPAA/HITECH notification duties to be deemed to have complied with the new notice content provisions under California law. Notification of the Attorney General must still be made if more than 500 California residents are affected by the breach, and all California notice duties would appear to apply to business associates under HIPAA.

• Businesses that provide notification under their own notice procedures as part of an information security policy are deemed to have complied with California notice requirements in total , so long as their internal procedures are “otherwise consistent with the timing requirements” of Civil Code §§ 1798.29 and 1798.82; i.e., notice is provided expediently and without unreasonable delay.

SB 24 was just approved on the Senate Floor by a vote of 34-4, has no formal opponents, and may go to the Governor’s desk by the end of the month, depending on the time needed to engross and enroll the bill. If the bill is not signed by September 9, Governor Brown will have an additional 30 days to sign it into law. Keep an eye out for a follow-up post confirming passage of the bill into law.

I:\cpr\Articles\California Legislature to Clarify Expand Data Breach Notice Requirements.doc
http://www.privacy.ca.gov/