Bloomberg BNA

Privacy and Security Law Report®



# Connecticut and Vermont Security Breach Amendments Demonstrate a Growing Trend: AG Notice Requirements

BY NATHAN D. TAYLOR

Since early May of this year, both Connecticut and Vermont amended their security breach notification laws to require notice to each state's respective state attorney general (AG) of data security breaches. The Connecticut and Vermont amendments and similar amendments made by other states last year demonstrate a growing national trend in state data security legislation—state reconsideration of, and ultimately amendments to, the requirements of existing state security breach notification laws.

## *Background*

Since California's landmark security breach notification law went into effect July 1, 2003, nearly every state has adopted a similar law. While the last state law to be enacted went into effect only last year (Mississippi), many, if not most, states enacted a law similar to the California law within five years. Today, 46 states, as well as the District of Columbia, Puerto Rico, and the U.S. Virgin Islands, have security breach notification laws on the books.

However, as time has passed and breach notices have proliferated across the country, however, many state legislatures have begun to consider new issues associated with security breach notification that likely were not considered at the time of enactment, such as the content that should be included in consumer notices, as well as whether any state regulator or agency, such as the state AG, should also be notified following a security breach.

As a result, the past several years have seen numerous bills introduced in state legislatures around the country that seek to amend existing state security breach notification laws. Although most of these bills have died at the end of state legislative sessions (much like Congress's nearly 10-year consideration of countless data security and security breach notification bills), some states have enacted amendments. For example, last year, three large states amended their security breach notification laws—California (to specify content requirements for consumer notices and to require notice to the California AG in certain instances), Texas (to provide that the state's consumer notice requirements apply with respect to covered personal information relating to Texas residents and to residents of any other state that does not require notice to individuals of a breach), and Illinois (to specify content requirements for consumer notices).

**One area in which a majority of state security breach notification laws are still silent is notice to state AGs or other authorities regarding a breach.**

In this regard, state amendments to breach laws appear to be a growing trend. One area in which a majority of state security breach notification laws are still silent is notice to state AGs or other authorities regarding a breach. As of the beginning of the year, of the 49 state security breach notification laws, only 14 states and Puerto Rico required notice to a state authority when a business was required to provide notice of a breach to the state's residents (California, Hawaii, Indiana, Louisiana, Massachusetts, Maryland, Maine, Missouri, New Hampshire, New Jersey, New York, Puerto Rico, South Carolina and Virginia). As a result, it seems likely that, to the extent a state legislature considers amendments

*Nathan D. Taylor is an associate with the Washington office of Morrison & Foerster, where he concentrates on assisting clients in managing consumer information, including customer and employee information, and developing procedures, practices, and other solutions to comply with complex privacy and information security laws.*

 ISSN 1538-3423

to an existing security breach notification law, the legislature will at least consider requiring notice to a state regulatory authority of security breaches. As discussed below, Connecticut and Vermont are the most recent states to make this type of amendment, but they will not likely be the last.

## *Connecticut*

On June 15, the Connecticut governor signed into law a seemingly innocuous state budget bill, H.B. 6001.[1] Buried within its nearly 500 pages was a section repealing the state's security breach notification law and replacing it with a substitute that was substantially similar to the existing law. The substitute, however, contains some new language. Of particular note, the bill will require, effective Oct. 1, 2012, that if a business is required to provide notice to Connecticut residents of a data security breach, the business also must notify the Connecticut AG. In this regard, the notice to the Connecticut AG must be provided no later than the time when notice is provided to Connecticut residents.

## *Vermont*

On May 5, 2012, the Vermont governor signed into law a bill, H. 254, that includes a provision requiring notice to the Vermont AG of data security breaches.[2]

Specifically, if a business[3] experiences a breach, the business must provide notice of the breach to the Vermont AG within 14 business days of discovering the breach or when the business provides notice to consumers, whichever is sooner. In this regard, the notice to the AG must include: (1) the date of the breach; (2) the date of discovery of the breach; (3) the number of Vermont consumers affected, if known; and (4) a copy of the notice provided to consumers.

H. 254, however, provides that a business that, prior to the breach, has sworn in writing to the AG (on a form and in a manner to be prescribed by the AG) that it maintains written policies and procedures to maintain the security of personally identifiable information and respond to a breach in a manner consistent with Vermont law may notify the AG of the breach prior to providing notice to consumers. This notice must include the date of the breach, the date of discovery of the breach, and a description of the breach. Although the law went into effect May 8, the form and the manner for making the sworn statement have not been published.

Nonetheless, a business will be able to obtain additional time before being required to notify the Vermont AG of a breach by having previously made a sworn statement to the AG regarding its information security and breach response policies. This fact will undoubtedly raise questions for many regarding whether it would be beneficial to make such a sworn statement; the answer, at least at this point, is not clear.

For example, until the Vermont AG actually issues the form on which the sworn statement will be made, the exact contours of the sworn statement (and related potential impact) will not be known. It is possible that the form could require a sworn statement that goes beyond the plain language of the statute, such as detailing specific types of information security policies and procedures (*e.g.*, encryption). It is also possible that the form could require documentation or proof of maintenance of written policies.

In addition, the implication of making a sworn statement to a state official that a business maintains certain policies and procedures should not be taken lightly. It is possible that the sworn statement could provide another avenue for enforcement relating to a company's failure to adequately protect personal information.

## *Practical Implications for Businesses*

It is important for businesses to keep in mind the existence of state AG breach notice requirements. If a business experiences a security incident that it thinks requires notice to consumers in one or more states, the business also must consider whether those states have notice requirements to the AG or another state entity. Moreover, it is important to keep in mind that the state AG notice requirements are far from uniform and require particular attention.

- For example, some states require that the state notice be provided within certain time frames, such as New Jersey, which requires notice to the state police prior to notifying consumers of the incident.
- Some states specify the contents of the AG notice, such as Massachusetts, which requires that the state notice include the nature of the breach, the number of Massachusetts residents affected at the time of notice, and any steps the business has taken or plans to take relating to the incident.
- California, New York and North Carolina require that the state notice be provided on a state-specific form or website.
- Some states require notice to the AG or other state entity only when the incident involves a certain number of state residents, such as California, which requires notice to the California AG only when notice will be provided to more than 500 California residents.

While Connecticut and Vermont may be the most recent states to adopt AG breach notice requirements, they undoubtedly will not be the last. Businesses should be cognizant of the ever-changing state landscape, and, in the event of the breach, determine any applicable requirements, such as notice to a state AG.

---

[1] H.B. 6001 is available at http://www.cga.ct.gov/2012/TOB/h/pdf/2012HB-06001-R00-HB.pdf.

[2] H. 254 is available at http://www.leg.state.vt.us/docs/2012/Acts/ACT109.pdf.

[3] In general, this requirement applies to any business that owns or licenses computerized personal information that includes personally identifiable information concerning a consumer that experiences a breach involving that information. The requirement, however, does not apply to a person who is licensed or registered under Title 8 of the Vermont Code by the Department of Financial Regulation.

  PVLR ISSN 1538-3423