THE
NATIONAL LAW REVIEW

Three Large States Revise Their Security Breach Notification Laws and Texas Applies Its Law to Residents of Some Other States to Boot

Wednesday, October 26, 2011

HUNTON ANDREWS KURTH

Article By Hunton Andrews Kurth
Jeff C. Dodd

Intellectual Property
Administrative & Regulatory
Texas
Illinois
California
All States
All Federal

Over forty states have adopted laws requiring businesses to implement some form of security procedures with respect to specified data relating to individuals[1] and to provide notice when those data security measures have been breached. While the structures of these laws often share common elements, the requirements vary somewhat. So, the problem for businesses is navigating the thicket of state laws when responding to data breaches potentially affecting the residents of several states. Three states—Texas, California and Illinois—recently amended their statutes. For those companies doing business across the United States that have comprehensive data notification plans, the changes are not so earth-shattering that your plans will change significantly (though you will need to address the particular changes). For those who do not have comprehensive plans, you will need to be aware that if you are afflicted with a breach, you will have to move quickly to assess your notification obligations under state laws that are stubbornly non-uniform.

Let us start with Texas. Before recent amendments, the Texas Business and Commerce Code required a "person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information" who suffers "any breach of system security"[2] to notify each "*resident of this state* whose *sensitive personal information*[3] was, or is reasonably believed to have been, acquired by an unauthorized person."[4] In essence, as with many states, the Texas notification statute required two ties to Texas for the statute to apply: the person with the notification duty had to conduct business in the state and the potentially affected persons had to be residents of Texas. Notice must be given as "quickly as possible" after "discovering or receiving notification of the breach,"[5] and the statute also sets forth acceptable manner of giving notice of the data breach.[6] Prior to recent amendments, the Texas statute imposed civil penalties for violations payable to the State of Texas of "at least $2,000 but not more than $50,000 for each violation."[7] In addition, a violation of the data notification statute is also "a deceptive trade practice actionable under Subchapter E, Chapter 17."

In 2011 Texas amended these provisions.[8] Most interestingly, Texas attempted to address one issue associated with a data breach potentially affecting residents of more than one state. Suppose, for example, a business does business in Texas and suffers a security breach affecting Texas residents and residents of another state that has no notification regime. The Texas legislature amended Texas law to make the notification obligation of a person conducting business in Texas run not only to any resident of Texas but also to any other resident in a state "that does not require" notification. If a state requires "a person described by Subsection (b)" to provide notice of a breach of system security, "the notice of the breach of system security provided under that state's law satisfies the requirements of Subsection (b)."

Here is the twist, however: Texas' statute may now reach, not only to the residents of states that have no notification statute, but also in one important set of circumstances to residents of those states that do. Bear with me here as I walk through the logic. A person "described by subsection (b)" is, presumably, a person "who

conducts business in [Texas] and owns or licenses computerized data." Many other states trigger notice obligations based when a person does business in their states, but the notice obligations run only to the residents of their states. Texas followed a similar approach before the amendments. Accordingly, before the amendments, if a company did business in Texas and suffered a security breach it had to notify residents of Texas, but the Texas statutes did not require notice to the residents of other states. That was left to other state law.

Now notice obligations run to all residents of all states as a threshold matter. Then in a new subsection (b-1), the amendments carve back on the scope of coverage: notice must be provided to residents of Texas and to residents of "another state that does not require a person described by Subsection (b)"—i.e. a person doing business in Texas owning or licensing computerized data—to provide notice of a security breach.[9] Clearly, if a company does business in Texas and in another state with a security breach notice statute, that company will be required to provide notice to potentially affected Texas residents under Texas law and notice to residents of the other state under the other state's law. Suppose, however, an enterprise does business in Texas and does not do business in another state (let us get creative and call it State X), but the residents of State X are potentially affected by the breach. If State X has a notification statute, but its statute has a double trigger—i.e., imposing obligations on the enterprise doing business in State X to provide notice to residents of State X—then technically a person doing business in Texas but not in State X would not be required to provide notice to residents of State X under State X's law. In that circumstance, as well as the situation where the other state has no breach notification law at all, the amendments to Texas law would require notice to potentially affected residents in the other states. We Texans are big-hearted enough to require notice to you even if your state does not.

The amendments also substantially increased the civil penalties for a failure to provide timely notice. *In addition to* the civil penalty payable to the State of Texas of "at least $2,000 but not more than $50,000 for each violation,"[10] the amended statute provides that "a person who fails to take reasonable action to comply with Section 521.053(b) is liable to this state for a civil penalty of not more than $100 for each individual to whom notification is due under that subsection *for each consecutive day that the person fails to take reasonable action* to comply with that subsection. Civil penalties under this section may *not exceed $250,000 for all individuals to whom notification is due after a single breach*."[11] Since this enhanced penalty is based on the number of individuals to which notice is not timely given, and since the statute now applies to at least some non-Texas residents, Texas may well collect for the alleged sins of Texas businesses affecting residents of other states.[12] We Texans are not only big-hearted, but we also know how to expand our revenue base. Bottom line: If you do business in Texas, it would pay to provide notice wherever you do business and to adopt policies that prescribe how notice will be given.[13]

California and Illinois also amended their data breach statutes to describe with some specificity what must go into the breach notices. California's law, as with Texas' law, applies to persons conducting business in its state but requires notice to be given only to California residents. In recent amendments to Section 1798.82 of its Civil Code, California tinkered with its notice requirements.[14] The notices must be written in "plain language"—I will defy you to cite an instance where a business issuing a notice says that it has written it in "unplain language"—and must set out the following:

- "The name and contact information of the reporting person or business."
- "A list of the types of personal information that were or are reasonably believed to have been the subject of a breach."
- If "possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice."
- "Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided."
- "A general description of the breach incident, if that information is possible to determine at the time the notice is provided."
- The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

The revised law also provides that at "the discretion of the person or business, the security breach notification may also include any of the following: (A) Information about what the person or business has done to protect individuals whose information has been breached and (B) Advice on steps that the person whose information has been breached may take to protect himself or herself." The problem, of course, is exactly what duties a business undertakes by setting out the protective measures it has taken and by providing advice as to protective measures.[15] Finally, the revised law requires that a sample copy of the notice be submitted to the California Attorney General if the notice is being required to be sent to more than "500 California residents as a result of a single breach of the security system."

Illinois also amended its statute this year to be more specific as to the notice requirements.[16] As amended, the law will require that notices to Illinois residents must "include, but need not be limited to, (i) the toll-free numbers and addresses for consumer reporting agencies, (ii) the toll-free number, address, and website address for the Federal Trade Commission, and (iii) a statement that the individual can obtain information from these sources about fraud alerts and security freezes."[17] Again, as I mentioned above, none of this is particularly earth-shattering and most data response plans would cover this type of information, but not all states require exactly the same type of information and so companies should take a look at their plans.

Also, prior to the amendments, data collectors maintaining data including personal information that they did not own or license had to notify owners or licensees of the data of a breach of its security measures. The amendments now require more of such service providers. "In addition to providing such notification to the owner or licensee, the data collector shall cooperate with the owner or licensee in matters relating to the breach. That cooperation shall include, but need not be limited to, (i) informing the owner or licensee of the breach, including giving notice of the date or approximate date of the breach and the nature of the breach, and (ii) informing the owner or licensee of any steps the data collector has taken or plans to take relating to the breach. The data collector's cooperation shall not, however, be deemed to require either the disclosure of confidential business information or trade secrets or the notification of an Illinois resident who may have been affected by the breach."[18] I note that the scope of the obligation to cooperate is not limited to the enumerated steps; rather the statute imposes a general, roving duty to cooperate.[19]

In the final analysis, the recent amendments to the Texas, California and Illinois security breach notification laws do not fundamentally change the way businesses that suffer a breach must approach giving notice of the breach, but the amendments underscore that each state may impose somewhat different obligations. Since the time to provide a notice is at a premium when a breach occurs (and since penalties can be quite heavy), we suggest that businesses operating in several states develop plans for compliance with the laws of those states before a breach occurs; for those with such plans in place, you should take a look at the new requirements to determine what, if anything, should be revised in your plans.

---

1. For example, Section 521.052 of the Texas Business and Commerce Code requires a business to "implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any *sensitive personal information* collected or maintained by the business in the regular course of business." Section 521.052(b) does not apply to "financial institutions" (as defined by 15 U.S.C. Section 6809) but, interestingly enough, it does apply to "a nonprofit athletic or sports association."

2. 521.053(a) of the Texas Business and Commerce Code provides that "breach of system security" means "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data."

3. "Sensitive personal information" is defined as an unencrypted first name or first initial of the first name with a last name in combination with one or more of the following: (a) social security number, driver's license number or government-issued identification number; (b) "account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account"; or information identifying an individual and relating to "the physical or mental health or condition of the individual," "the provision of health care to the individual," or "payment for the provision of health care to the individual." Texas Business and Commerce Code Section 521.002(a).

4. 521.053(c) also provides that any "person who maintains computerized data that includes sensitive personal information not owned by the person shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

5. Prompt notice is excused to the extent necessary "to determine the scope of the breach and restore the reasonable integrity of the data system" or to the extent requested by "a law enforcement agency that determines that the notification will impede a criminal investigation."

6. 521.053(e) sets forth methods for providing notice, but 521.053(g) provides businesses with discretion to set their own procedures: "Notwithstanding Subsection (e), a person who maintains the person's own notification procedures as part of an information security policy for the treatment of sensitive personal information that complies with the timing requirements for notice under this section complies with this section if the person notifies affected persons in accordance with that policy."

7. Section 521.151 of the Texas Business and Commerce Code clearly vests the discretion in the Texas Attorney

General as to whether to bring the action. It also allows the Texas Attorney General to see equitable relief and to recover reasonable expenses.

8. H.B.ANo.A300. The amendments take effect September 1, 2012. http://www.capitol.state.tx.us/tlodocs/82R/billtext/pdf/HB00300F.pdf#navpanes=0

9. Here is the new exception in full:

> (b-1) Notwithstanding Subsection (b), the requirements of Subsection (b) apply only if the individual whose sensitive personal information was or is reasonably believed to have been acquired by an unauthorized person is a resident of this state or another state that does not require a person described by Subsection (b) to notify the individual of a breach of system security. If the individual is a resident of a state that requires a person described by Subsection (b) to provide notice of a breach of system security, the notice of the breach of system security provided under that state's law satisfies the requirements of Subsection (b).

Texas Business & Commerce Code 521.053(b-1)(effective September 1, 2012).

10. Section 521.151(a) of the Texas Business and Commerce Code.

11. Texas Business & Commerce Code 521.053(b-1) (effective September 1, 2012).

12. Texas also extensively revised its Health and Safety Code requirements as to data security and privacy to reach beyond the obligations of the Health Information Portability and Accountability Act.

13. As I mentioned above, Texas Business & Commerce Code 521.053(g) provides businesses with discretion to set their own procedures: "Notwithstanding Subsection (e), a person who maintains the person's own notification procedures as part of an information security policy for the treatment of sensitive personal information that complies with the timing requirements for notice under this section complies with this section if the person notifies affected persons in accordance with that policy."

14. Senate Bill No. 24, Chapter 197, approved by the Governor of California on August 31, 2011. http://www.infolawgroup.com/uploads/file/sb_24_bill_20110831_chaptered.pdf.

15. Consider the following question: By stating that a notice "may" include such other information, does the statute imply that the prescribed and identified permissive information is the only information that can be included in a notice?

16. HB 3025, Public Act 097-0483. http://www.ilga.gov/legislation/fulltext.asp?GAID=11&SessionID=84&GA=97&DocTypeID=HB&DocNum=3025&LegID=60509&SpecSess=&Session= In addition to the amendments summarized above, the statute imposes specific obligations concerning the disposal of data containing personal information. Several states have that requirement.

17. HB 3025, Public Act 097-0483, Section 10(a). Interestingly, the statute adds that the "notification shall not, however, include information concerning the number of Illinois residents affected by the breach."

18. HB 3025, Public Act 097-0483, Section 10(b).

19. The amendments do not speak to cost reimbursement.

Copyright © 2019, Hunton Andrews Kurth LLP. All Rights Reserved.

Source URL: https://www.natlawreview.com/article/three-large-states-revise-their-security-breach-notification-laws-and-texas-applies-its-law-