A Publication of Law Bulletin Publishing Company
Chicago Lawyer®
Info Tech Law

Data breach notice laws are changing

November 2011

BY ALAN S. WERNICK, ESQ.
T: 847.786.1005 – E: ALAN@WERNICK.COM

State data breach laws have proliferated: 46 states plus the District of Columbia all have their own data breach notification laws. California, the first state to enact a data breach notification law, recently passed new changes to its data breach statute.

For several years Congress attempted to pass a national data breach notification law. Presently, three separate data breach notification bills are pending in Congress. What do the data breach notification law changes portend for businesses and their legal advisers?

When a business is a victim of a data breach it must (in addition to the investigation, remediation and other tasks) comply with the applicable data breach notification laws or risk the consequences for failing to comply. Perhaps the biggest consequence to the business is the loss of trust by the customers of the business — as they suddenly face the risk of being victims of identity theft because of the data breach. This consequence is in addition to the potential civil penalties and undertakings that may be imposed on the business as a result of the breach, depending on the applicable data breach law.

Additionally, with the number of applicable data breach notification laws presently enacted in the U.S., a substantial burden today on a business responding to a data breach is the cost of determining which of the current many different data breach laws apply and how to respond.

In my December 2006 article titled "Data theft and state law" I noted that "the California data breach notification law … is one of the first of such statutes in the United States and the one other states and Congress have considered in the drafting of similar legislation." That article identifies the numerous different types of Personal Identifiable Information (PII) represented by the many different data breach notification statutes at that time. It also provides details about PII and the impacts PII has on the business' duty to notify.

Which applicable data breach notification applies will be determined by the facts of the data breach including the state of residency of the individuals affected by the data breach. Thus, if a business based in Illinois has customers who reside in California, then the California data breach notification laws may be implicated in the event of a data breach affecting those California customers.

In the recent changes to its data breach notification laws (effective Jan. 1 of next year), California now requires businesses, depending on the facts of the data breach, to provide notice to the state's attorney general's office and the California Office of Privacy Protection and to provide to those entitled to receive notice of the data breach certain information about the breach.

In addition, the new California statute changes the substitute notice provisions for those breaches requiring notice to about 500,000 state residents or costing about $250,000 to send individual notices. Now the California data breach notification statute (§1798.29 and §1798.82) requires substitute notice to include: a) e-mail notice when the business has an e-mail address for the subject persons; b) conspicuous posting of the notice on the website page of the business, if the business maintains one; and c) notification to major statewide media and (as applicable as per the statute) the Office of Information Security within the California Technology Agency or the Office of Privacy Protection within the State and Consumer Services Agency — thus adding additional notification requirements. A covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act, is deemed to have complied only with the notice provisions (§1798.82(d)) of the data breach notification law if it has complied with existing federal law, as specified in the new statute.

Regarding the data breach notification bills (S. 1151, S. 1408, and S. 1535) presently pending in Congress, they would pre-empt the state data breach notification laws and eliminate the burden of uncertainty on businesses trying to determine which applicable state data breach law applies. Some of the differences among the bills include (and may be amended or eliminated in the final version):

- Different triggers for data breach notification;
- Criminal penalties for intentionally concealing a data breach;
- Special rules for the data broker industry; and
- Allowing the Federal Trade Commission to write rules for data security programs. (Note, the FTC has been one of the most proactive federal agencies in effectively addressing data breaches and has spearheaded a number of consumer and business education awareness initiatives regarding data breach and identity theft.)

A national data breach law may help reduce uncertainty and costs for businesses when they deal with a data breach. Whether Congress is able to communicate, collaborate and cooperate in working through the issues and apply the necessary critical thinking to produce a national data breach law is yet to be seen.