Connecticut May Require Businesses to Offer Identity Theft Protection Services Following a Data Breach

By Joseph J. Lazzarotti

June 3, 2015

Following other states that have toughened their data breach notification laws, Connecticut is about to amend its law to require that businesses provide one year of identity-theft protection for persons affected by a data breach, among other things.

Many businesses already extend such services to victims of a data breach. However, if enacted, Connecticut's Senate Bill 949 would mandate covered businesses incur this expense. Connecticut Attorney General George Jepsen said this change would set only "a floor for the duration of the protection" and his office may continue to "seek broader kinds of protection," reports the Hartford Courant.

Senate Bill 949 would require those conducting business in the state and who own or license certain personal information of a Connecticut resident that is involved in a data breach to:

offer to each resident...appropriate identity theft prevention services and, if applicable, identity theft mitigation services. Such service or services shall be provided at no cost to such resident for a period of not less than twelve months. Such person shall provide all information necessary for such resident to enroll in such service or services and shall include information on how such resident can place a credit freeze on such resident's credit file.

Projected to become effective October 1, 2015, the bill also would require notice be provided no later than 90 days from discovery of the breach. The law currently requires notification without unreasonable delay. Other provisions of the bill would add data security requirements applicable to state agencies and companies that contract with the state.

If signed by Governor Dannel Malloy, Senate Bill 949 would add another state law to those that businesses already must contend with when they experience multi-state data breaches. The frequently changing laws (highlighted by the Connecticut bill and others summarized below) underscore the need for companies to plan a response to possible data breaches. According to InfoSecurity Magazine, about 86 percent of IT executives "feel prepared" for a data breach, but only 40 percent have a response plan. A company's IT Director may feel she is prepared from an information security perspective, but may not have considered the steps the company would have to take in the event of a breach. These may include:

- investigation,
- notification,
- legal compliance,
- media relations,
- coordination with law enforcement,
- arranging for identity theft protection services, and
- setting up a call center.

Changes in Other States

A number of states have strengthened their breach notification laws. Some have added provisions specifically for states agencies, while others have revised data security mandates concerning student data. For example, Virginia enacted H.B. 2350 to direct the state's Department of Education to develop a model data security plan that may be used by school divisions to implement policies and procedures related to the protection of student data and data systems.

Meet the Author

Joseph J. Lazzarotti

Principal
Berkeley Heights 908-795-5205
Email

Montana: Beginning October, certain medical information will be added to the definition of personal information that could trigger data breach notification. That definition includes first name or initial and last name together with social security number, driver license number, or certain financial account numbers. The amendment also requires notification to the State's Attorney General's office, as well as the affected individuals.

Nevada: Effective July 1, the personal information that will trigger the notification requirement if breached includes (i) a medical identification number or a health insurance identification number, and (ii) a user name, unique identifier or electronic mail address in combination with a password, access code, or security question and answer that would permit access to an online account.

North Dakota: Effective on and after August 1, businesses no longer have to be doing business in the state to be subject to the law. They simply have to own or license personal information that belongs to a resident of the state. The amended law also adds a notification requirement to the state's Attorney General if more than 250 residents are affected by the data breach. Other changes also were made to the law.

Washington: Effective July 24, Washington's breach notification law will include: (i) a 45-day deadline for providing notification; (ii) a requirement to notify the state Attorney General; (iii) specific notice content requirements, such as the name and contact information of the business reporting the breach; and (iv) expanded application of the law to personal information in paper format.

Wyoming: Effective July 1, the elements of personal information that would trigger breach notification and the information that must be included in the notification letters will be changed by two amendments, S.F. 35 and S.F. 36. Under the law as amended, personal information also includes personal data such as: (i) federal- or state-government issued identification card; (ii) shared login secrets or security tokens known to be used for data-based authentication; (iii) username or email address in combination with a required password or security question and answer; (iv) a birth or marriage certificate; and (v) certain medical and health insurance information. Notifications must provide breach victims specific information such as: (i) the types of personal identifying information believed to have been the subject of the breach; (ii) a general description of the breach and the approximate date of the breach, if reasonably possible to determine at the time of the notice; (iii) actions taken to protect the system from further breaches; and (iv) advice directing affected persons to remain vigilant by reviewing account statements and monitoring credit reports.

For additional information and assistance with these and other laws, please contact a member of our Privacy, e-Communication and Data Security practice or the Jackson Lewis attorney with whom you regularly work.