Client Alert: Delaware Adds New Cybersecurity Requirement and Expands Data Breach Notification Regulations

Related Professionals

John L. Landolfi

Christopher L. Ingram

Related Services

Data Strategy, Privacy and Security

CLIENT ALERT | 8.23.2017

Companies doing business in Delaware should be aware of a recent amendment to its cybersecurity and data breach notification law. Effective April 14, 2018, companies will be required to ensure that reasonable procedures and practices are in place to protect Delaware residents' personal information collected through the course of business. This new law does not define or otherwise elaborate on the specific procedures or practices that will be deemed acceptable.

The amendment also adds more stringent requirements to Delaware's existing data breach notification law. Importantly, companies will be required to provide one year of free credit monitoring to affected individuals if a data breach involves their social security numbers. However, there is an exception to this potentially costly requirement. A company will not be required to provide credit monitoring services if, after an appropriate investigation, the company determines it is unlikely any harm will result to individuals whose information was part of the breach.

Additionally, the law expands the types of information that triggers Delaware's notification requirement. Existing law defined "personal information" to include an individual's name combined with either a social security number, a driver's license number, or financial account information. The amendment expands this definition to also include an individual's name in combination with medical information, health insurance information, biometric data, a user name or email address (with information sufficient to gain access to that account), passport number, and taxpayer identification number.

The amendment also clarifies when notice to affected individuals must be provided. Companies will be required to notify Delaware residents affected by a data breach within 60 days after a determination that a breach has occurred unless a delay is warranted by an ongoing criminal investigation. Finally, for any breach affecting more than 500 Delaware residents, companies will now be required to notify the state attorney general of the breach no later than when the notice is provided to affected individuals.

Companies that conduct business in Delaware or collect personal information from Delaware residents should evaluate their data breach incident response plans to incorporate these changes. These companies should also review the cybersecurity practices and procedures for guarding individuals' personal information to ensure that they will withstand scrutiny. For questions on cybersecurity programs, breach response, breach preparedness or planning, please contact John Landolfi, Chris Ingram or your Vorys attorney.