Florida Overhauls Data Breach Notification Law

June 25, 2014

Last Friday, Florida enacted a new Information Security Act that repeals the state's existing data breach notification law and increases companies' reporting obligations and liability in the event of a data security breach. The new law takes effect July 1, 2014. Likely in response to the recent high-profile breaches, several states have introduced legislation to strengthen existing data security laws, and it is important for companies to monitor these developments and assess and revise information security policies, as necessary.

The new law will require regulator notice (written notice to the Department of Legal Affairs) if more than 500 Florida residents are affected by a breach, as well as if a company reasonably determines that notice is not required because the breach has not resulted, and will not likely result, in identity theft or other financial harm. Additionally, the new law specifies the content that must be included in both the consumer and regulator notice; imposes a 30-day timeframe for covered entities to provide such notice; and revises the definition of personal information to include medical and health insurance information and an individual's user name or email address in combination with the required password or security question and answer. Furthermore, the law requires that third-party agents notify a company of a breach of security within 10 days, and, although the third-party agent may provide the required notice, the company is ultimately responsible for any failure by the agent to provide proper notice.

Importantly, the new law codified the Act within Florida's Deceptive and Unfair Trade Practices Act, and specifies that a violation of the Information Security Act constitutes an unfair or deceptive trade practice. Under the DUTPA, the Attorney General may bring actions for a declaratory judgment, injunction, or actual damages. These remedies are in addition to the civil penalties the Department may assess, up to $500,000, for failure to comply with the consumer and regulator notice requirements.