CLIENT ALERT

Florida Paves the Way For More Stringent State Data Breach Laws

Jun.26.2014

Following on the heels of several high-profile data breaches, on June 20, 2014, Florida strengthened its breach notification law. The Florida Information Protection Act of 2014 (FIPA), which takes effect July 1, will become one of the most aggressive breach laws in the country by shortening the reporting time to thirty days and adding several information classes that trigger notification obligations when breached. The amendment comes at a time when state regulators are moving to strengthen data protection laws, and federal regulators – such as the FTC and HHS – are increasingly flexing their regulatory authority to punish companies for data breaches. FIPA therefore serves as a reminder that companies must monitor the rapidly evolving patchwork of data laws and update their policies and incident response plans accordingly. Perhaps more importantly, FIPA also is an indicator that states may continue to enact increasingly stringent laws in the absence of comprehensive national breach legislation.

In 2005, Florida was only the tenth state to enact a breach notification law. Now, almost ten years later, its recent amendment has overhauled the steps both commercial and governmental entities must take in response to a security breach. The FIPA changes are significant:

- "Personal Information" Definition Broadened. FIPA broadens the definition of "personal information" to include health insurance and medical information, joining the relatively few states with a similar definition such as California, Arkansas, Missouri, North Dakota, and Texas. The amended definition also now covers user names and e-mail addresses, when disclosed in combination with security information such as passwords that would permit account access, joining California and North Carolina.
- Reporting Time Frame Narrowed. Florida now has the shortest breach reporting deadline of any state that sets a limit by statute. Entities must provide notice "as expeditiously as possible" but in no event later than thirty days after either the discovery of the breach or a reasonable belief that a breach has occurred (shortening the previous 45 day time limit).
- Reporting to State Regulators and CRAs Now Required. Under FIPA, entities must report breaches affecting 500 or more individuals in the state to Florida's Department of Legal Affairs. Entities must also report breaches affecting more than 1,000 individuals to the major Consumer Reporting Agencies (CRAs). Here, too, reporting is required within a short timeframe – no later than thirty days after the discovery of a breach.
- "Reasonable Measures" to Protect Data Required. FIPA also includes a new requirement that entities use "reasonable measures" to protect and secure data containing personal information in electronic form. Like many other states that require such "pre-breach" security measures, FIPA does not specify what such "reasonable measures" may entail.

Despite the numerous revisions that Florida has codified in FIPA, the state has maintained certain aspects of its original data breach law that may provide some comfort:

- "Risk of Harm" Trigger Maintained. Contrary to other laws that no longer contain a "risk of harm" threshold for notification – such as the Health Insurance Portability and Accountability Act (HIPAA) – FIPA continues to maintain a "risk

of harm" trigger before notice to the individual is required. Thus, notification to individuals is not required if it has been reasonably determined that the breach has not and will not result in any form of financial harm, including identify theft. However, this is complicated by the fact that such risk determinations can only be made after an appropriate investigation and consultation with relevant law enforcement agencies. These determinations must also be in writing, maintained for five years, and provided to the Department within thirty days of finalization.

- Administrative Penalties Not Increased. FIPA does not increase the administrative penalties first laid out in 2005, which are capped at $500,000 per breach (as opposed to per individual). Like most other states, FIPA also does not provide a private cause of action to individuals.

Additionally, in conjunction with signing FIPA into law, Governor Scott signed a second bill that exempts certain kinds of FIPA reports from public disclosure. Information submitted to the Department under FIPA that includes personal data, forensic reports, or that "would otherwise reveal weaknesses in a covered entity's data security" are not subject to public records requests. By expressly exempting certain information from public disclosure, Florida has sought to address a common concern among companies: how to provide information to regulators without risking another breach if that information were disclosed. This provision will also take effect on July 1.

Overall, the FIPA amendments make clear that companies are expected to provide prompt and comprehensive notifications to individuals affected by a security breach. Given the proliferation of data breaches, and the increasing focus on cybersecurity at the state and federal levels, the trend to strengthen cybersecurity and breach notification laws will likely continue.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Jeffrey L. Poston
Partner – Washington, D.C.
Phone: +1 202.624.2775
Email: jposton@crowell.com

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com

Kate M. Growley, CIPP/G, CIPP/US
Partner – Washington, D.C.
Phone: +1 202.624.2698
Email: kgrowley@crowell.com