PUBLICATION

Alabama's Data Breach Notification Law Takes Effect June 1, 2018

April 12, 2018

On March 28, Alabama Governor Kay Ivey signed SB 318, the Alabama Data Breach Notification Act of 2018, which becomes effective on June 1, 2018. Alabama was the final state to enact a data breach notification law, and many have referred to Alabama's Act as one of the most stringent in the United States in many different areas. Key takeaways from the Act include:

- The Act only applies to electronic data, and includes an encryption safe harbor in the event of a "breach;"
- Notice to residents must be provided "as expeditiously as possible and without unreasonable delay," but no later than 45 days after a breach is discovered if it is reasonably likely to cause substantial harm, with specific information included within the notice;
- The term "Covered entities" includes government agencies, but exempts financial institutions and other businesses that are subject to federal guidelines governing data breach notification, provided that they are meeting the requirements of their regulatory authority and the institution notifies Alabama's Attorney General when the number of individuals impacted by a breach exceeds 1,000;
- An entity must designate "an employee or employees to coordinate" data security measures, implement and maintain "reasonable security measures" to protect personal information in the event of a breach, and keep management – including a board of directors – informed of its security measures;
- The Act expands the definition of "personal information" to include health information and a username or email address in combination with a password;
- A private right of action is not provided, but the Attorney General may enforce the Act in a "representative capacity" on behalf of individuals affected by the breach in an action for damages, including reasonable attorneys' fees and costs; and
- The Act allows civil penalties of not more than $5,000 per day to be assessed to entities that fail to take reasonable action to comply with the notice provisions of the Act, while a knowing or reckless disregard in failing to comply with the notice requirements could subject covered entities to fines up to $500,000 per breach.

Although 14 other states have enacted stand-alone statutory obligations to maintain reasonable cybersecurity measures, Alabama's Act provides specific factors that would be used to evaluate whether a covered entity's security measures are "reasonable," including that the measures be "practicable . . . to implement and maintain." Entities must also identify internal and external cyber risks; adopt appropriate information safeguards to address those risks; contract with service providers that are required to maintain appropriate safeguards; and continually evaluate and adjust their security measures as circumstances change according to the entity's size, amount of information stored, and the costs associated with implementing and maintaining its security measures.

Alabama's Act also provides guidance on information governance protocols within a mandate that covered entities and third-party service providers "take reasonable measures" to dispose of records containing sensitive, personally identifying information when those records "are no longer to be retained pursuant to applicable law, regulations, or business needs."

Nearly every type of business is captured by the Act's definition of "covered entity," defined as a "person, sole proprietorship, partnership, government entity, corporation, non-profit, trust, estate, cooperative association, or other business entity" under the Act. As a result, businesses that acquire or maintain sensitive, personally identifying information for Alabama residents should immediately review their current information governance and incident response plans with their legal counsel to ensure compliance with the Act.

If you have further questions on how the Alabama Data Breach Notification Act will affect your organization, please contact any member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team.