BURR ALERT 2018

Alabama Has Joined the Party – What Your Business Needs to Know about Alabama's New Data Privacy Law

By India E. Vincent April 2018

On March 28, 2018, Alabama adopted a data privacy law, the Alabama Data Breach Notification Act of 2018 (SB318). While Alabama is one of the last states to adopt such an act, the Act is notable in its requirements, and applies to any "person, sole proprietorship, partnership, government entity, corporation, nonprofit, trust, estate, cooperative association, or other business entity" that acquires, has possession of, or uses Sensitive Personally Identifying Information. The stated objective of the breach is protecting the data of Alabama residents, and it defines a breach as the "unauthorized acquisition of data in electronic form containing sensitive personally identifying information."

While data privacy laws certainly are not new at this point, there are likely many businesses in Alabama who have thus far not had to focus on compliance with requirements as strict as those set forth in the Act, including how the business stores, manages, uses, and destroys its data and how the business responds to a security incident. With the June 1st effective date quickly approaching, businesses who have not previously taken steps to assess their data security plans need to do so now. Given the scope of the Act, except for those excepted businesses, almost all businesses in Alabama will be impacted by at least part of this Act.

The first step is to understand the data that a company brings in from all data sources (employees, customers, vendors and others), where that data is stored, how it is stored, how it is used, who has access, why it is collected and how long it is retained. Once a business has that information it can begin developing plans and implementing processes to ensure compliance with this Act.

The key objective to minimize liability under this Act, or others like it, is not to store information that is not needed for the business purpose. If a business currently retains information that is not part of the business process, identify that data now and take steps to remove it from the records using proper methods. Then focus on the remaining data, its sensitivity and what needs to be done to protect it. This will vary for every business, and most businesses with limited in-house IT and legal assistance will need the assistance of consultants to help with expediting this process. If information must be stored, proper consideration for encryption, truncation or other means to prevent the data from being used if it is acquired by an unauthorized user may be effective security measures for some businesses, but those measures should be carefully evaluated to ensure they are sufficient because other measures may be needed as well.

Beyond the collection, storage and use of the data, businesses must have a firm understanding of what they will do in the event of a breach. With the requirements to conduct a good faith and

prompt investigation and to notify affected individuals as "expeditiously as possible, without unreasonable delay," businesses can't afford to wait until the breach occurs to figure out what to do. Knowing ahead of time who will take the lead in an incident investigation, who will be the decision maker(s), who will be responsible for re-securing the system, who will be responsible for assessing the scope of the intrusion, and who will be responsible for preparing the necessary notices, can make the difference in whether or not a business can meet the requirements of this Act. Another key factor for businesses is assessing agreements with their vendors and other service providers who may have access to Sensitive Personally Identifiable Information and ensuring that those third parties are in compliance with the Act and are contractually obligated to provide notice to the business in the required time frames so that the business may then meet its own reporting requirements.

The good news for those businesses that are already regulated under federal laws, or those businesses regulated under state laws that have protections and reporting requirements at least as strict as this Act, is they are not subject to the Act, provided they comply with existing requirements.

A full summary of the provisions of the Act can be accessed here; however, a few of the key highlights are as follows:

- Sensitive Personally Identifying Information is defined to include an individual Alabama resident's first name or initial and last name in combination with one or more pieces of information, including as examples, social security numbers, driver's license numbers, banking account numbers, health insurance numbers, email address or physical addresses.
- The Act enumerates factors to be considered when determining if the security efforts are reasonable, and those include whether someone in the organization is identified as responsible for data security issues, whether the risks and safeguards are assessed, and whether management is kept informed on these issues.
- Identified issues that are recurring and/or systemic weigh more heavily against the reasonableness of the security measures.
- Reporting requirements are triggered if the entity knows information has been acquired or reasonably believes the information has been required and is likely to cause substantial harm.
- An incident can trigger a reporting requirement even if the data is not transferred out of the company's system, if the unauthorized person had access to the data, with factors for determining access specified in the Act.
- There are specific requirements for personal notices in the event of a breach, and if the company does not have such information it may be required to provide substitute notice through means of public notice of the breach. It is important to make sure business records are complete (or are purged if not necessary), so that personal notices can be provided if necessary.
- If a business experiences an incident and decides not to notify, it must retain its records documenting that decision for no less than 5 years.

Compliance with these requirements may be daunting for businesses who have not yet had to venture down this path, but with some attention and planning, businesses of all sizes and resources can meet the requirements set forth in this Act.

If you would like more information on how to prepare for the effective date of the Alabama Data Breach Notification Act of 2018, please contact:

India E. Vincent in Birmingham at ivincent@burr.com or (205) 458-5284

or the Burr & Forman attorney with whom you regularly work.