ALABAMA DATA BREACH NOTIFICATION ACT

EFFECTIVE GUIDANCE AND MEASURES TO KEEP YOUR COMPANY PROTECTED

Failure to follow items noted in this law could result in fines and fees for the business of up to $500,000.
This document points out methods to follow to help protect the information of your customers and employees.

On March 28, 2018, Alabama became the 50th state to enact a breach notification law with the passing and signing of the Alabama Data Breach Notification Act of 2018 (2018-396) (the Act). This Act requires a business entity that "acquires or uses sensitive personally identifiable information" to have certain security measures in place to help prevent a cybersecurity breach from occurring, as well as certain response and notification measures to alert affected individuals of the breach or cybersecurity event within a reasonable amount of time.

Sensitive personally identifiable information relates to (1) non-truncated or non-encrypted social security numbers, tax IDs, drivers licenses, (2) financial institution account numbers in connection with security access codes and passwords, (3) medical history or diagnosis, (4) health insurance numbers or IDs or (5) a user name or email address in connection with a password or security question and answer. Already made public information is exempt from this definition, along with truncated, encrypted, secured or securely removed elements of the identity of the individual.

The Alabama Data Breach Notification Act of 2018 has two fundamental elements: measures to prevent a breach from occurring and steps to take if a breach occurs. Security measures to implement are applicable to all companies, but the steps to take if a breach occurs will vary depending on the scope of the breach and how many individuals were affected.

Companies that work in cyberspace face a never-ending barrage of potential

SECURITY ATTACKS

from a growing list of internal and external risks.

WARREN AVERETT'S RECOMMENDATIONS BASED ON THE ACT'S REQUIREMENTS:

- An individual or a group within your organization should be designated as the Information Security Officer or the Information Security Committee or have an equivalent title.
- An annual risk assessment should be completed for the entire organization, or at least the IT department.
- Your organization should have solid information technology and security controls in place to

(continued)

Warren Averett
CPAs AND ADVISORS

prevent breaches/incidents. Use the risks that your company identifies in itself to identify areas of concern, and respond to those by implementing provisions that will reduce or eliminate your risk.

- Ensure that your organization has a thorough understanding of what pieces of sensitive information each of your vendors has access to and what they are doing with them.
- Your organization should have all security measures reviewed periodically and be able to change those controls around sensitive information and data.
- Outside of governmental entities, an organization's information security department needs to communicate clearly to the Board of Directors/ Management about security strength and ensure this communication reaches any internal committees that oversee IT risk and security.

OTHER ITEMS TO NOTE CONCERNING THE ACT

The Act also requires that companies properly dispose of information that is no longer needed by your business or legally required to be retained, and fines and penalties are subject to be given to those organizations that are not in compliance with the provisions presented in this Act.

WHAT TO DO

Because each company will have different needs, it is important to fully understand how the Act will specifically and uniquely impact your company. And because all breaches are different, and the Act requires different steps depending on the breadth and impact of the breach, it is also important to know how your company would respond to such an event and how to be prepared.

STEPS TO TAKE IF A BREACH OCCURS:

1. Conduct an investigation of the breach to determine the effects, including what information was involved, whether the information is in the possession of an unauthorized party, what repercussions may be and how to reestablish effective security.
2. In light of the results of the findings of an investigation, your company may need to take some or all of the following steps:
   - notify the individuals affected within 45 days according to specific stipulations concerning the communication of such
   - provide written notice to the Attorney General (if the breach impacts more than 1,000 people)
   - contact consumer reporting agencies (if the breach impacts more than 1,000 people)
   - pursue appropriate documentation.

Depending on your company's function and the details of the breach, you may need to notify others as early as 10 days after a breach has been discovered.

For additional information related to this Act and to learn how Warren Averett may be able to help your organization meet these requirements or respond to a breach, please contact Paul Perry at Paul.Perry@warrenaverett.com.

Warren Averett
CPAs AND ADVISORS