OF THE ALABAMA DATA BREACH NOTIFICATION ACT OF 2018:

Will Your Company Be Compliance Ready by June 1, 2018?

By Daniel Fortune, Jeremy Gaddy and Bart Cannon, Huie, Fernambucq & Stewart

GOVERNOR IVEY RECENTLY SIGNED the Alabama Data Breach Notification Act of 2018 into law. The Act, which goes into effect June 1, 2018, is intended to protect Alabama residents from Breaches of data that is stored or used by Covered entities. The Act requires any person or company who acquires or uses sensitive personally identifying information to not only implement security measures to protect the data, but also to assess its data security measures and to provide certain notices if there is a breach. The reality is nearly all companies in Alabama will be required to comply with the Act when it goes into effect on June 1, 2018.

In February 2018, Kaspersky Labs issued the "Spam and Phishing in 2017 Report" that indicated phishing attacks increased by 59 percent in 2017. Similarly, according to the "2017 Verizon Data Breach Investigation Report", 61 percent of breaches involved businesses with less than 1,000 employees. The construction industry includes many small and mid-size businesses with limited resources for cybersecurity; however, something as simple as an employee responding to a phishing email may be considered a data breach and may trigger compliance requirements under the Act. As construction companies increasingly use computers, smartphones, and other smart equipment to conduct business, vulnerability to breaches and liability for the unauthorized disclosure of a customer's sensitive personally identifying information also increases. Anyone in the construction industry that collects or uses customer information should plan to protect that information with cybersecurity procedures and organize an Incident Response Plan to comply with the new Alabama Data Breach Notification Act of 2018.

HERE IS AN OVERVIEW OF THE ABCs AND 123s TO REMEMBER AS WE APPROACH JUNE 1, 2018:

A Alabama residents and their sensitive personally identifying information are protected by the Act, which includes the following: social security numbers, tax identification numbers, driver's license numbers, information regarding individual's medical treatment, an individual's health insurance policy number, an email address and password that would permit access to an online account, and financial account numbers or credit cards in conjunction with passwords or login information that would allow access to those accounts.

B Breach protection, investigation, notification, and remedies are mandated by the Act. The Act mandates companies implement and maintain reasonable cybersecurity measures. It also establishes remedies for breaches and prescribes possible penalties for anyone who fails to comply.

Before any incident, companies must 1) identify internal and external risks of breaches; 2) adopt appropriate information safeguards to address identified risks and assess the effectiveness of the information safeguards; and, 3) retain service providers that are contractually required to maintain information safeguards.

If a company determines that a breach has or may have occurred, it must conduct a prompt, good faith investigation. In doing so, the entity must 1) assess the nature and scope of the breach and determine whether the breach is reasonably likely to cause substantial harm to affected individuals; 2) identify and implement measures to restore the security and confidentiality of the compromised systems; and, 3) notify all affected individuals as expeditiously as possible and without unreasonable delay but not later than 45 days after believing a breach has occurred. A business must also notify the Alabama Attorney General if more than 1,000 individuals are involved. The notice to the individuals must include 1) a synopsis of the events surrounding the breach; 2) the approximate number of affected individuals; and, 3) any services being offered without charge to the individuals and related instructions.

A violation of the notice provision of the act is a violation of the Alabama Deceptive Trade Practices Act which can be prosecuted by the Attorney General's Office for civil penalties against the Covered Entity.

C Covered Entity is broadly defined, with a few exceptions, as anyone, or any corporation, or other business entity who acquires or uses sensitive personally identifying information in Alabama.

Benjamin Franklin is often credited with saying, "if you fail to plan, you are planning to fail." If your company acquires or uses sensitive personally identifying information, time is running short to ensure you have a plan that complies with the requirements of the Act and that reasonably protects your company and the data it maintains.

Start planning now. The Alabama Data Breach Notification Act of 2018 goes into effect on June 1, 2018.