HAND ARENDALL HARRISON SALE LLC

CYBERSECURITY Alert

Alabama Data Breach Notification Act of 2018

On March 28, 2018, Alabama Governor Kay Ivey signed into law the Alabama Data Breach Notification Act of 2018, making Alabama the fiftieth state to enact such legislation into law. Earlier in March, South Dakota enacted a similar law, making Alabama the only state in the country, until now, without a mandatory notification law following a data breach. The Alabama Data Breach Notification Act of 2018 ("the Act") is similar to several other states' mandatory notification laws. The Act becomes effective June 1, 2018. Some of the key provisions of the Act include the following:

- The Act defines "sensitive personally identifying information" ("PII") to include specific combinations of an Alabama resident's name and other personal information such as a social security number, driver's license number, personal medical information, certain financial account information, and even certain electronic information like a username and password. The Act specifically defines what information is considered sensitive PII governed by the Act.

- The Act applies to any "covered entity", which is defined to include any business entity, governmental entity, nonprofit, trust, estate, or association that acquires or uses sensitive PII.

- The Act also applies to a third-party agent of a covered entity that is responsible for maintaining, storing, or accessing sensitive PII. These third-party agents must notify a covered entity within ten (10) days of discovery of a suspected breach, and must cooperate with the covered entity to facilitate any mandatory disclosure under the Act. Failure of the third-party agent to comply with the obligations of the Act may subject the third-party agent to penalties.

- Each covered entity and third-party agent must implement and maintain "reasonable security measures" to protect sensitive PII from a potential breach.

- If a breach has occurred or is suspected to have occurred, "a good faith and prompt investigation" must occur to determine if sensitive PII "has been acquired or is reasonably believed to have been acquired by an unauthorized person, and is reasonably likely to cause substantial harm to the individuals to whom the information relates."

This alert was prepared by Hand Arendall Harrison Sale's Cybersecurity Practice Group. For further information or assistance, please contact any member of the practice group below.

George M. Walker
Practice Group Chair
gwalker@handarendall.com
251-694-6296

Practice Group Members:

Brett W. Aaron
Roger L. Bates
Joseph L. Cowan
Kelly Thrasher Fox
Christopher M. Gill
C. Dennis Hughes
Jason E. Lee
Sarah Outlaw McLaughlin
J. Burruss Riis
Jack P. Russell
Christopher S. Williams

- If the notification requirement is triggered, the Act sets forth certain mandatory obligations with deadlines and exceptions for notification of the affected individuals. Subject to certain exceptions, notification must be made within forty-five (45) days of the discovery of the breach. Additional requirements apply to a breach involving more than one thousand (1,000) individuals' PII.

- Violation of the notification requirements of the Act does not constitute a criminal offense and does not establish a private civil cause of action. Under the Act, the Alabama Attorney General has the exclusive authority to bring an action for civil penalties, and the Attorney General can recover actual damages for individuals, plus reasonable attorney's fees and costs.

- A violation of the notification provision of the Act can result in a civil penalty of $5,000 **per day** for every day the party fails to comply with the notice provisions of the Act. A knowing violation of the notification provisions of the Act can result in penalties up to $500,000 per breach.

- The Act requires a covered entity or third-party agent to take "reasonable measures" to dispose of records containing sensitive PII when the records are no longer required to be retained pursuant to applicable law.

Members of the Hand Arendall Harrison Sale cybersecurity practice group can advise on the implementation of "reasonable security measures" to avoid a data breach, and ensure "reasonable measures" are in place to dispose of records containing sensitive PII. We can also assist in the investigation of a suspected breach, provide legal advice on whether notification is required, and make other recommendations related to compliance with the Alabama Data Breach Notification Act of 2018.

If you have any questions about the Act, or would like information about Hand Arendall Harrison Sale's cybersecurity flat fee packages, please contact Christopher S. Williams.