The Alabama Data Breach Notification Act of 2018

Edward A. "Ted" Hosp
Maynard, Cooper & Gale, PC
thosp@maynardcooper.com
334-233-7157

Senate Bill 318 was introduced by Senator Arthur Orr (R-Decatur) on Tuesday, February 13, 2018. It was revised significantly at every stage of the legislative process before receiving final passage on March 27. The bill was signed by Governor Kay Ivey on March 28, and became Act 2018-396. ***The new law goes into effect on June 1.***

The primary intent of the legislation, and one could argue the only true effect, is to require timely notice to affected individuals when their personal information has been compromised, and to provide an enforcement mechanism for the Attorney General when a business fails to provide that notice.

Only the failure to notify affected individuals and, if the breach affects more than 1,000 Alabama residents, the Attorney General of a breach subjects an entity to penalties under the Act. That said, there still are actions that businesses are "required" to take under other provisions of the new law.

I. What Entities are Covered?

- A "covered entity" is a person or a business of any kind that acquires and maintains "Sensitive Personally Identifying Information" ("SPII").

II. What Data is Considered "Private"(SPII)?

- SPII includes non-truncated (*i.e.*, non-shortened or partially redacted) identifying codes or account numbers combined with the person's first name or initial and their last name. These include:
    - Social Security number or tax ID number;
    - Driver's license number, state-issued identification card number, passport number, military identification number;
    - Bank account number, credit card number, or debit card number (in combination with any security code, access code, password, expiration date, or PIN);
    - Information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis;
    - An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual;
    - A user name or email address (in combination with a password or security question and answer that would permit access to an online account).

III. Evaluation and Implementation of Security Systems

- Covered entities must conduct an assessment of their data security, and then establish reasonable security measures to protect SPII from being breached.
- What is "reasonable" is expressly tied to the relative size of the entity as well as the amount and type of SPII in its possession. Also relevant to what is reasonable for a business to implement is the cost that would be incurred to put in place and to maintain a security program.
- In implementing a system of security, the Act instructs entities to consider all of the following:

1. Designation of an employee or employees to coordinate the covered entity's security measures to protect against a breach of security. An owner or manager may designate himself or herself;
2. Identification of internal and external risks of a breach of security;
3. Adoption of appropriate information safeguards to address identified risks of a breach of security and assess the effectiveness of such safeguards;
4. Retention of service providers, if any, that are contractually required to maintain appropriate safeguards for sensitive personally identifying information;
5. Evaluation and adjustment of security measures to account for changes in circumstances affecting the security of sensitive personally identifying information;
6. Keeping the management of the covered entity, including its board of directors, if any, appropriately informed of the overall status of its security measures.

- Businesses also must take reasonable steps when disposing of SPII to mitigate the risk that it falls into the wrong hands.

IV. What is a Breach?

- A breach is the unauthorized acquisition of data in electronic form containing sensitive personally identifying information (SPII).

IV. What is Required After a Breach?

A. Good Faith Investigation and Evaluation

- An entity that has suffered a breach must conduct a "good faith and prompt investigation" to determine:
    1. The scope of the breach;
    2. Whose information was compromised, and the nature of that information;
    3. Whether the breached information is "reasonably likely to cause substantial harm" to the person; and
    4. Measures to be taken to restore security of the information and system breached.
- Factors to consider in determining if a breach is "reasonably likely to cause substantial harm:"
    1. The information is in the physical possession of an unauthorized person;
    2. The information has been copied or downloaded;
    3. The information has been used by an unauthorized person; and/or
    4. The breached information has been made public.
- A business must maintain detailed records of its activities following a breach for five (5) years.

B. Notice to Affected Individuals

- An entity that has suffered a breach that is "reasonably likely to cause substantial harm" must give individual notice of the breach to those affected.
- Notice must be given "as expeditiously as possible and without unreasonable delay" but in no event more than 45 days from the determination of the breach.
- The time to inform individuals (and the Attorney General under Section 6) begins to run from the date of the determination that the breach is "reasonably likely to cause substantial harm" and not from the date of the determination of the occurrence of the breach.
- Notice can (and should) be delayed when requested by federal or state law enforcement based on a criminal investigation or national security issues.
- Individual notice must be in writing and must include the following:

1. The date of the breach;
2. The information that was breached;
3. The action taken to restore the confidentiality of the data;
4. The actions that a person can take to protect himself/herself from the breach; and
5. Information about how to contact the covered entity with questions.

- A business may be entitled to use substitute (non-individual) notice under the following circumstances:
  1. Insufficient information regarding the affected individuals;
  2. Excessive cost to provide notice relative to the size and resources of the business;
  3. The breach affected more than 100,000 Alabama residents; ***or***
  4. Where the cost of notice would exceed $500,000
- Generally, substitute notice requires the business to:
  1. Post a conspicuous notice of the breach on its website for at least 30 days; and
  2. Place notice of the breach in print and broadcast media where affected individuals reside.
- BUT: the Attorney General has the authority to approve a different method of substitute notice requested by the business.

C. Notice to the Attorney General

- Written notice to the Attorney General is required when the breach affects more than 1,000 Alabama residents.
- Notice to the Attorney General must be made "as expeditiously as possible" but in no event more than forty-five (45) days after the determination that the breach is "reasonably likely to cause substantial harm."
- **NOTE**: do not confuse the individual notice requirements with the requirement to notify the Attorney General.
  - Notice of a breach is ALWAYS required to the affected individuals - even if only one person is affected.
  - Notice to the Attorney General is only required if more than 1,000 Alabama residents are affected.
- Notice to the Attorney General must include:
  1. A description of the "events surrounding the breach;"
  2. The number of people affected;
  3. Services being offered to those affected by the breach; and
  4. Contact information for a point person regarding the breach.
- Information provided to the Attorney General that is marked as confidential is not subject to any open records or freedom of information request.

D. Notice to Credit Reporting Agencies

- A breach in excess of 1,000 persons also requires notice to"all consumer reporting agencies."

V. What if a Third Party Vendor Suffers a Breach?

- A third party agent that suffers a breach must notify the covered entity of the breach within 10 days.
- The third party must provide the business with "information in the possession of the third-party agent so that the covered entity can comply with its notice obligations."
- The covered entity must conduct an evaluation of the breach and provide the notice to affected individuals, the AG and consumer credit reporting agencies as described above within forty-five (45) days.
- The time for a covered entity to provide notice begins to run when the covered entity receives notice of the breach from that third party entity.
- The business, not the third party is required to provide notice, but the parties may enter into a contractual arrangement that shifts the burden to the third party.

VI. Penalties and Enforcement

- There are two provisions in ACT 2018-396 under which an entity could face penalties for failure to provide notice:
    1. If a failure to provide notice is "willful or with reckless disregard," then the penalty provisions of the Alabama Deceptive Trade Practices Act would apply.
        - Penalties under the DTPA can be imposed at $2,000 per violation (per person), but penalties are capped in the bill at $500,000.
        - Violation is not a criminal offense and the criminal provisions of the Alabama Deceptive Trade Practices Act (DTPA),
    2. An entity that continues to fail to comply with the notice provisions past the forty-five (45) day deadline can be fined up to $5,000 per day.
- The heightened culpability standard and cap on DTPA penalties are important changes from prior years' proposals.
- No private right of action - the Act states that it does not create a private cause of action.
- The Attorney General has exclusive authority to bring an action on behalf of individuals but only for actual damages..
    - NOTE: This provision may allow the Attorney General to pursue an action against an entity for the breach itself - rather than for a failure to notify.

VII. Entities Subject to Federal or Other Alabama Data Breach Standards

- Entities subject to federal data breach standards (*e.g.* Gramm-Leach-Bliley, HIPAA), that comply with those standards and provide notice of a breach pursuant to those standards are exempt from the Alabama Act.
- BUT - they must also provide a copy of the notice to the Attorney General.
- An entity subject to an Alabama data breach and notification provision that is at least as stringent as SB318, need only comply with that law, without regard to the requirements of SB318.