Publications
May 17, 2018
SECURITY BREACH NOTIFICATION CHART - Alabama

Ala. Stat. § 8-38-1 *et seq.*

Alabama S.B. 318 (signed into law March 28, 2018)

Effective June 1, 2018

Application. A person or commercial entity (collectively, Entity) that acquires or uses sensitive personally identifying information.

Security Breach Definition. The unauthorized acquisition of data in electronic form containing sensitive personally identifying information.

- Good-faith acquisition of sensitive personally identifying information by an employee or agent of an Entity is not a security breach, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.
- A security breach also does not include the release of a public record not otherwise subject to confidentiality or nondisclosure requirements, nor does it include any lawful, investigative, protective, or intelligence activity of a law enforcement or intelligence agency of the state, or a political subdivision of the state.

Notification Obligation. Notice is required to affected AL residents if the Entity determines that, as a result of a breach of security, personal information has been acquired by an unauthorized person and is reasonably likely to cause substantial harm.

Notification to Consumer Reporting Agencies. If an Entity is required to notify more than 1,000 AL residents of a breach, the Entity shall also notify without unreasonable delay all nationwide consumer credit reporting agencies of the timing, distribution, and content of the notices to AL residents.

Attorney General/Agency Notification. If the number of individuals requiring notice exceeds 1,000, the Entity must notify the Attorney General as expeditiously as possible and without unreasonable delay, and within 45 days once it is determined that a breach has occurred and is reasonably likely to cause substantial harm to affected individuals. Written notice must include:

- A synopsis of the events surrounding the breach
- The number of affected individuals in AL.
- Any services related to the breach being offered or scheduled to be offered, without charge, by the Entity to individuals, and instructions as to how to use such services.
- The name, address, telephone number, and email address of the employee or agent of the Entity from whom additional information may be obtained about the breach.

Third-Party Data Notification. Any third-party agent shall disclose to the Entity for which the information is maintained, any breach of the security of the system as soon as practicable, but no later than 10 days following the determination of the breach or reason to believe the breach occurred. Upon receiving notice from a third-party agent, the Entity shall provide notices to the Attorney General and affected individuals. A third-party agent must provide the Entity with all information that the Entity needs to comply with notice requirements. A third-

party agent may contract with the Entity whereby the third-party agent agrees to handle required notifications.

Timing of Notification. Notice shall be made as expeditiously as possible and without unreasonable delay, taking into account the time necessary to conduct an investigation, and within 45 days of discovering that a breach has occurred and is reasonably likely to cause substantial harm to affected individuals.

Personal Information Definition. An AL resident's first name or first initial and last name, in combination with one or more of the following data elements:

- Social Security number;
- Tax identification number;
- Driver's license number or state identification card number, passport number, military identification number, or other unique identification number issued on a government document used to verify the identity of a specific individual;
- Account number, credit card number, or debit card number in combination with any required security code, access code, password, expiration date, or PIN, that is necessary to access the financial account or to conduct a transaction that will credit or debit the financial account;
- Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;
- An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual; or
- A username or email address, in combination with a password or security question and answer that would permit access to an online account affiliated with the Entity that is reasonably likely to contain or is used to obtain sensitive personally identifying information.

Personal information does not include information about an individual that is lawfully made public by a federal, state, or local government record or widely distributed media.

Personal Information does not include information that is truncated, encrypted or otherwise rendered unusable, unless the encryption key or other credential necessary to render the information usable has also been compromised.

Notice Required. Notice may be provided by one of the following methods:

- Written notice; or
- Email notice.

Notice must contain, at a minimum:

- The date, estimated date, or estimated date range of the breach.
- A description of the PI that was acquired.
- A general description of the actions taken by the Entity to restore the security and confidentiality of the PI.
- A general description of the steps the affected individuals can take to protect themselves from identity theft.
- Contact information for the Entity where individuals can inquire about the breach.

Substitute Notice Available. If the Entity demonstrates (a) excessive cost (greater than $500,000 or excessive relative to the Entity's resources); (b) more than 100,000 persons are affected, or (c) the Entity does not have sufficient contact information to provide notice. Substitute notice shall include both of the following:

- Conspicuous posting of the notice on the website of the Entity if the Entity maintains one, for a period of 30 days; and
- Notice to major print and broadcast media, including major media in urban and rural areas where the affected individuals reside.

Exception: Compliance with Other Laws.

- An Entity is exempt from this chapter if it:
    - Is subject to or regulated by (a) federal laws, rules, regulations, procedures, or guidance *or* (b) state laws, rules, regulations, procedures, or guidance that are at least as thorough as the notice requirements in this law; and
    - Maintains procedures pursuant to those requirements; and
    - Provides notice to consumers pursuant to those requirements, and
    - Timely provides notice to the Attorney General when the number of affected individuals exceeds 1,000.

Other Key Provisions:

- **Delay for Law Enforcement.** Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation or national security, and the law enforcement agency has submitted a written request for the delay. The law enforcement agency may revoke the delay as of a specified date or extend the delay, if necessary.
- Government entities are subject to the Act as well and must provide notice in line with the provisions of the law.
- **Attorney General Enforcement.** The Attorney General has exclusive authority to bring an action for civil penalties under the Act.