

Alabama

AL ST §§ 8-38-1, *et seq.*

Quick Links

[Statute](#)

[AG Website](#)

Quick Facts

Is “Personal Information” broader than the general definition? ¹	✓ Yes
Does the law apply to paper records?	✗ No
Is notification triggered by access only?	✗ No
Is a risk-of-harm analysis permitted?	✓ Yes
Is notice to a state agency or AG required?	✓ Yes, if 1,000 or more residents receive notice
Is there a specific deadline for individual notices?	✓ Yes
Is there a specific format or language that must be included in the individual notice?	✓ Yes
Is notice to consumer reporting agency?	✓ Yes, if more than 1,000 Alabama residents are notified
Is a private right of action permitted?	✗ No

“Breach” Definition

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

“Personal Information” Definition

1. An individual’s first name or first initial and last name in combination with one or more of the following:
 - a. A nontruncated Social Security number or tax identification number
 - b. A nontruncated driver’s license number, state-issued 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

¹ The general definition of “Personal Information” is an individual’s name in combination with any one or more of the following: (1) Social Security number; (2) driver’s license number or state identification card number; or (3) a financial account number or credit or debit card number in combination with any required security code, access code, or password that is necessary to permit access to an individual’s financial account.

- c. A financial account number, including a bank account number, credit card number, or debit card number, in combination with any 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
- d. Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional
- e. 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
- f. 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 covered entity that is reasonably likely to contain or is used to obtain sensitive personally identifying information.

Notification Trigger

Following investigation:

1. Following notification from a third-party agent that a breach has occurred, or determination that a breach is likely to cause substantial harm to individuals, entity that owns or licenses computerized personal information shall notify Alabama residents within 45 days.
2. Entity that only maintains, stores or processes computerized personal information shall notify the owner or licensee of the breach as expeditiously as possible and without unreasonable delay, but no later than 10 days following the determination or belief that a breach has occurred.

Risk-of-Harm Analysis Standard

Notification is not required if, after a reasonable investigation, it is determined that there is no reasonable likelihood of causing substantial harm to consumers.

Alabama law outlines four factors to consider when determining whether personal information has been acquired.

Special Form/Content of Consumer Notice

The notice shall include:

1. The date, estimated date, or estimated date range of the breach
2. A description of the sensitive personally identifying information that was acquired by an unauthorized person as part of the breach
3. A general description of the actions taken by a covered entity to restore the security and confidentiality of the personal information involved in the breach
4. A general description of steps an affected individual can take to protect himself or herself from identity theft; and
5. Information that the individual can use to contact the covered entity to inquire about the breach

AG Notice Trigger/Deadline

If the number of individuals an entity is required to notify exceeds 1,000, the entity shall notify the attorney general as expeditiously as possible and without unreasonable delay, but no later than 45 days after the

entity either (i) determines that a breach is reasonably likely to cause substantial harm to individuals; or (ii) receives notice from a third-party agent that a breach has occurred.

Notification to Consumer Reporting Agencies Threshold

If an entity discovers circumstances requiring notice to more than 1,000 individuals, the entity shall also notify, without unreasonable delay, all consumer reporting agencies.