Publications
June 01, 2014

SECURITY BREACH NOTIFICATION CHART - Georgia

Ga. Code § 10-1-910 ***et seq.***

S.B. 230 (signed into law May 5, 2005)

Effective May 5, 2005

S.B. No. 236 (signed into law May 24, 2007)

Effective May 24, 2007

Application. Any person or entity who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing PI to nonaffiliated third parties, or any state or local agency or subdivision thereof including any department, bureau, authority, public university or college, academy, commission, or other government entity (collectively, Entity) that maintains computerized data that includes PI of individuals.

- The statute shall not apply to any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes or for purposes of providing public access to court records or to real or personal property information.

Security Breach Definition. An unauthorized acquisition of an individual's electronic data that compromises the security, confidentiality, or integrity of PI of such individual maintained by an Entity.

- Good-faith acquisition or use of PI by an employee or agent of an Entity for the purposes of such Entity is not a breach of the security of the system, provided that the PI is not used or subject to further unauthorized disclosure.

Notification Obligation. Any Entity that maintains computerized data that includes PI of individuals shall give notice of any breach of the security of the system following discovery or notification of the breach to any resident of GA whose unencrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Notification to Consumer Reporting Agencies. In the event an Entity discovers circumstances requiring notification of more than 10,000 residents of GA at one time, the Entity shall also notify, without unreasonable delay, all nationwide consumer reporting agencies of the timing, distribution, and content of the notices.

Third-Party Data Notification. Any person or business that maintains computerized data on behalf of an Entity that includes PI that the Entity does not own, it shall notify the other Entity of any breach of the security of the system within 24 hours following discovery if the PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Timing of Notification. In the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

Personal Information Definition. An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

- Social Security number;
- Driver's license or state identification card number;
- Account number, credit card number, debit card number if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords;
- Account passwords or personal identification numbers or other access codes; or
- Any of the above items when not in connection with the individual's first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.

PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

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

- Written notice;
- Telephone notice; or
- Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-Sign Act).

Substitute Notice Available. If an Entity demonstrates that the cost of providing notice would exceed $50,000, that the affected class of individuals to be notified exceeds 100,000, or that the Entity does not have sufficient contact information to provide written or electronic notice to such individuals. Substitute notice shall consist of all of the following:

- Email notice, if the Entity has email addresses for the individuals to be notified;
- Conspicuous posting of the notice on the Entity's website, if the Entity maintains one; and
- Notification to major statewide media.

Exception: Own Notification Policy. Any Entity that maintains its own notification procedures as part of an information security policy for the treatment of PI and whose procedures are otherwise consistent with the timing requirements of the statute shall be deemed to be in compliance with the notification requirements of the statute if it notifies the individuals who are the subjects of the notice in accordance with its policies in the event of a breach of the security of the system.

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. Notice required by the statute must be made without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation.