

SECURITY BREACH NOTIFICATION CHART - Louisiana

La. Rev. Stat. § 51:3071 *et seq.*

La. Admin. Code tit. 16, pt. III, § 701

S.B. 205 (signed into law July 12, 2005, Act 499)

Effective January 1, 2006

S.B. 361 (signed into law May 16, 2018, Act 382)

Effective August 1, 2018

Application. Any individual, any legal entity that conducts business in LA, or any agency, that owns or licenses computerized data that includes PI (collectively, Entity).

Security Breach Definition. The compromise of the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to PI maintained by an Entity.

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

Notification Obligation. An Entity shall notify any resident of the state whose PI was, or is reasonably believed to have been, acquired by an unauthorized person.

- Notification is not required if after a reasonable investigation the Entity determines that there is no reasonable likelihood of harm to LA residents. The Entity shall retain a copy of the written determination and supporting documentation for 5 years and provide a copy to the Attorney General upon request.

Attorney General Notification. When notice to LA citizens is required by the statute, the Entity shall provide written notice detailing the breach of the security of the system to the Consumer Protection Section of the Attorney General's Office. Notice shall include the names of all LA citizens affected by the breach. Notice to the state Attorney General shall be timely if received within 10 days of distribution of notice to LA citizens.

Third-Party Data Notification. Any individual, corporation, partnership, sole proprietorship, joint stock company, joint venture, or any other legal entity that maintains computerized data that includes PI that the agency or person does not own shall notify the owner or licensee of the information if the PI was, or is reasonably believed to have been, acquired by an unauthorized person through a breach of security of the system containing such data, following discovery by the agency or person of a breach of the security system.

Timing of Notification. In the most expedient time possible and without unreasonable delay, but not later than 60 days from discovery of the breach, consistent with any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system. When notification is

delayed by law enforcement request or due to a determination by the Entity that measures are necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system, the Entity shall provide the Attorney General the reasons for the delay in writing within the 60-day notification period. Upon receipt of the written reasons, the Attorney General shall allow a reasonable extension of time to provide the consumer notification.

Personal Information Definition. The first name or first initial and last name of a LA resident in combination with any one or more of the following data elements, when the name or the data element is not encrypted or redacted:

- Social Security number;
- Driver's license number or state identification card number;
- Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account;
- Passport number; or
- Biometric data. "Biometric Data" means data generated by automatic measurements of an individual's biological characteristics, such as fingerprints, voice print, eye retina or iris, or other unique biological characteristic that is used by the owner or licensee to uniquely authenticate an individual's identity when the individual accesses a system or account.

"Personal information" shall 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 notification; or
- Electronic notification, if the notification 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 notification would exceed \$100,000, or that the affected class of persons to be notified exceeds 100,000, or the Entity does not have sufficient contact information. Substitute notice shall consist of all of the following:

- Email notification, when the Entity has email addresses for the subject persons;
- Conspicuous posting of the notification on the Entity's website, if the Entity maintains one; and
- Notification to major statewide media.

Exception: Own Notification Policy. Any Entity that maintains notification procedures as part of its information security policy for the treatment of PI that 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 the Entity notifies the subject persons in accordance with the policy and procedures in the event of a breach of a security of the system.

Exception: Compliance with Other Laws.

- **Federal Interagency Guidance.** A financial institution that is subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, and any revisions, additions, or substitutions relating to said interagency guidance, shall be deemed to be in compliance.

Penalties.

- A civil action may be instituted to recover actual damages resulting from the failure to disclose in a timely manner to a person that there has been a breach of the security system resulting in the disclosure of a person's PI.
- Failure to provide timely notice may be punishable by a fine not to exceed \$5,000 per violation. Notice to the state Attorney General shall be timely if received within 10 days of distribution of notice to LA citizens. Each day that notice is not received by the state Attorney General shall be deemed a separate violation.

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.
- **Private Right of Action.** A civil action may be instituted to recover actual damages resulting from the failure to disclose in a timely manner to a person that there has been a breach of the security system resulting in the disclosure of a person's PI.