RS 51:3074

§3074. Protection of personal information; disclosure upon breach in the security of personal information; notification requirements; exemption

A. Any person that conducts business in the state or that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information, shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

B. Any person that conducts business in the state or that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information shall take all reasonable steps to destroy or arrange for the destruction of the records within its custody or control containing personal information that is no longer to be retained by the person or business by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.

C. Any person that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information, shall, following discovery of a breach in the security of the system containing such data, notify any resident of the state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

D. Any agency or person that maintains computerized data that includes personal information that the agency or person does not own shall notify the owner or licensee of the information if the personal information 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 security of the system.

E. The notification required pursuant to Subsections C and D of this Section shall be made in the most expedient time possible and without unreasonable delay but not later than sixty days from the discovery of the breach, consistent with the legitimate needs of law enforcement, as provided in Subsection F of this Section, or any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system. When notification required pursuant to Subsections C and D of this Section is delayed pursuant to Subsection F of this Section or due to a determination by the person or agency that measures are necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system, the person or agency shall provide the attorney general the reasons for the delay in writing within the sixty day notification period provided in this Subsection. Upon receipt of the written reasons, the attorney general shall allow a reasonable extension of time to provide the notification required in Subsections C and D of this Section.

F. If a law enforcement agency determines that the notification required under this Section would impede a criminal investigation, such notification may be delayed until such law enforcement agency determines that the notification will no longer compromise such investigation.

G. Notification may be provided by one of the following methods:

(1) Written notification.

(2) Electronic notification, if the notification provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. 7001.

(3) Substitute notification, if an agency or person demonstrates that the cost of providing notification would exceed one hundred thousand dollars, or that the affected class of persons to be notified exceeds one hundred thousand, or the agency or person does not have sufficient contact information. Substitute notification shall consist of all of the following:

(a) E-mail notification when the agency or person has an e-mail address for the subject persons.

(b) Conspicuous posting of the notification on the Internet site of the agency or person, if an Internet site is maintained.

(c) Notification to major statewide media.

H. Notwithstanding Subsection G of this Section, an agency or person that maintains a notification procedure as part of its information security policy for the treatment of personal information which is

otherwise consistent with the timing requirements of this Section shall be considered to be in compliance with the notification requirements of this Section if the agency or person notifies subject persons in accordance with the policy and procedure in the event of a breach of security of the system.

I. Notification as provided in this Section shall not be required if after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to the residents of this state. The person or business shall retain a copy of the written determination and supporting documentation for five years from the date of discovery of the breach of the security system. If requested in writing, the person or business shall send a copy of the written determination and supporting documentation to the attorney general no later than thirty days from the date of receipt of the request. The provisions of R.S. 51:1404(A)(1)(c) shall apply to a written determination and supporting documentation sent to the attorney general pursuant to this Subsection.

J. A violation of a provision of this Chapter shall constitute an unfair act or practice pursuant to R.S. 51:1405(A).

Acts 2005, No. 499, §1, eff. Jan. 1, 2006; Acts 2018, No. 382, §1.