§ 3071. Short title

This Chapter may be cited as the “Database Security Breach Notification Law”.

§ 3072. Legislative findings

The legislature hereby finds and declares that:

(1) The privacy and financial security of individuals are increasingly at risk due to the ever more widespread collection of personal information.

(2) Credit card transactions, magazine subscriptions, telephone numbers, real estate records, automobile registrations, consumer surveys, warranty registrations, credit reports, and Internet web sites are all sources of personal information and form the source material of identity theft.

(3) The crime of identity theft is on the rise in the United States. Criminals who steal personal information use the information to open credit card accounts, write bad checks, buy automobiles, and commit other financial crimes using the identity of another person.

(4) Identity theft is costly to the marketplace and to consumers.

(5) Victims of identity theft must act quickly to minimize the damage; therefore, expeditious notification of possible misuse of a person's personal information is imperative.

§ 3073. Definitions

As used in this Chapter, the following terms shall have the following meanings:

(1) “Agency” means the state, a political subdivision of the state, and any officer, agency, board, commission, department or similar body of the state or any political subdivision of the state.

(2) “Breach of the security of the system” means the compromise of the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable likelihood to result in, the unauthorized acquisition of and access to personal information maintained by an agency or person. Good faith acquisition of personal information by an employee or agent of an agency or person for the purposes of the agency or person is not a breach of the security of the system, provided that the personal information is not used for, or is subject to, unauthorized disclosure.

(3) “Person” means any individual, corporation, partnership, sole proprietorship, joint stock company, joint venture, or any other legal entity.

(4)(a) “Personal information” means the first name or first initial and last name of an individual resident of this state in combination with any one or more of the following data elements, when the name or the data element is not encrypted or redacted:

(i) Social security number.

(ii) Driver's license number or state identification card number.

(iii) Account number, credit 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.

(iv) Passport number.

(v) 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.

(b) “Personal information” shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

§ 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).

§ 3075. Recovery of damages

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 personal information.

§ 3076. Financial institution; compliance

A financial institution that is subject to and in compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer 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 with this Chapter.