

CHAPTER 51. DATABASE SECURITY BREACH NOTIFICATION LAW

§3071. Short title

This Chapter may be cited as the "Database Security Breach Notification Law".  
Acts 2005, No. 499, §1, eff. Jan. 1, 2006.

## §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.

Acts 2005, No. 499, §1, eff. Jan. 1, 2006.

## §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 basis to conclude has resulted 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 an individual's first name or first initial and last name 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.

(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.

(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.

Acts 2005, No. 499, §1, eff. Jan. 1, 2006.

§3074. 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, 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.

B. 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.

C. The notification required pursuant to Subsections A and B of this Section shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in Subsection D 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.

D. 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.

E. 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 USC 7001.

(3) Substitute notification, if an agency or person demonstrates that the cost of providing notification would exceed two hundred fifty thousand dollars, or that the affected class of persons to be notified exceeds five 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.

F. Notwithstanding Subsection E 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 deemed 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.

G. Notification under this title<sup>1</sup> is not required if after a reasonable investigation the person or business determines that there is no reasonable likelihood of harm to customers.

Acts 2005, No. 499, §1, eff. Jan. 1, 2006.

<sup>1</sup>As appears in enrolled bill. Should be "Section".

§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.

Acts 2005, No. 499, §1, eff. Jan. 1, 2006.

§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.

Acts 2005, No. 499, §1, eff. Jan. 1, 2006.