SLS 18RS-605 **ORIGINAL**

2018 Regular Session

SENATE BILL NO. 361

BY SENATOR WALSWORTH

ATTORNEY GENERAL. Provides relative to the protection of computerized data that contains personal information and requires notification of data breaches. (8/1/18)

AN ACT

To amend and reenact R.S. 51:3073(4)(a) and 3074, relative to the Database Security Breach Notification Law; to provide for the protection of personal information; to require certain security procedures and practices; to provide for notification requirements; to provide relative to violations; to provide for definitions; and to provide for related matters.

Be it enacted by the Legislature of Louisiana:

Section 1. R.S. 51:3073(4)(a) and 3074 are hereby amended and reenacted to read as follows:

§3073. Definitions

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

* * *

(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 **or state identification card**.

(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.

* * *

§3074. ~~Disclosure~~ **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 though any means.

C. 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.~~**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.

~~C.~~**E.** The notification required pursuant to Subsections ~~A and B~~ **C and D** of this Section shall be made in the most expedient time possible and without unreasonable delay **but not later than forty-five days**, consistent with the legitimate needs of law enforcement, as provided in Subsection ~~D~~ **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.

~~D.~~**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.

~~E.~~**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 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.~~**H.** Notwithstanding Subsection ~~E~~ **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 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 is not required if after a reasonable investigation the person or business determines that there is no reasonable likelihood of harm to customers.~~

I. Violations of any of the provisions of this Chapter shall constitute an unfair practice under R.S. 51:1405(A).

The original instrument and the following digest, which constitutes no part of the legislative instrument, were prepared by Curry Lann.

DIGEST

SB 361 Original 2018 Regular Session Walsworth

Present law defines "personal information" as 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:

(1) Social security number.

(2) Driver's license number.

(3) 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.

Proposed law defines "personal information" as 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:

(1) Social security number.

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

(3) 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.

(4) Passport number.

(5) Biometric data.

Proposed law requires 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, to 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.

Proposed law requires 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 to 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.

Present law requires notification to be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system.

Proposed law retains present law and further requires that notification be made within 45 days.

Present law provides that notification is not required if after a reasonable investigation the person or business determines that there is no reasonable likelihood of harm to customers.

Proposed law repeals present law.

Present law (R.S. 51:1405(A)) declares unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce unlawful.

Proposed law retains present law and provides that violations of the Database Security Breach Notification Law constitute an unfair practice under R.S. 51:1405(A).

Effective August 1, 2018.

(Amends R.S. 51:3073(4)(a) and 3074)