SLS 16RS-197 **ORIGINAL**

2016 Regular Session

SENATE BILL NO. 103

BY SENATOR JOHN SMITH

INSURANCE COMMISSIONER. Provides for notification to the commissioner of insurance of breaches of data security in systems containing certain personal information relating to consumers. (8/1/16)

AN ACT

To amend and reenact R.S. 44:4.1(B)(11) and to enact R.S. 22:51, relative to notification to the commissioner of insurance of breaches of data security; to provide for reporting by regulated persons; to provide for the information to be reported; to provide for exceptions; to provide for penalties; to provide for corrective actions; and to provide for related matters.

Be it enacted by the Legislature of Louisiana:

Section 1. R.S. 22:51 is hereby enacted to read as follows:

§51. Data system breach notification to the commissioner

A. For the purposes of this Section, the following terms shall have the following meanings:

(1) "Breach" or "data breach" means the compromise of the security, confidentiality, or integrity of computerized data that results in, or that there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to personal information or protected health information. Good faith acquisition of personal information or protected health information by an employee or agent of a person regulated by the department or of a third-party

service provider of a person regulated by the department is not a breach of the security of the system, provided that the information is not used for or subject to unauthorized disclosure.

(2) "Encryption" or "encrypted" means the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key.

(3) "Person" has the same meaning as provided in R.S. 22:46.

(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:

(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.

(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.

(5) "Protected health information" has the same meaning as provided in 45 C.F.R. 160.103.

(6) "Redacted" means altered or truncated so that no more than the last four digits of a Social Security number, driver's license number, state identification card number, account number, or credit or debit card number is accessible as part of the data.

(7) "Regulated by the department" means required to be licensed or registered by, to apply for a certificate of authority from, or to submit to an examination by the Louisiana Department of Insurance.

(8) "Third-party service provider" means a person who provides services to a person regulated by the department in connection with a product or service

offered by the person regulated by the department and who accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses the personal information or protected health information of Louisiana residents as a result of such services.

B.(1) Any person regulated by the department who owns or licenses computerized data shall notify the commissioner following the discovery of a breach in the security of any data processing system containing the personal information or protected health information of one or more residents of Louisiana, regardless of whether or not the data belonging to the Louisiana residents has actually been compromised.

(2) Any person regulated by the department shall notify the commissioner if the person discovers or is notified of a breach in the security of a data processing system of a third-party service provider that contains the personal information or protected health information of one or more residents of Louisiana, regardless of whether or not the data belonging to the Louisiana residents has actually been compromised.

(3) Any person regulated by the department and legally domiciled or having its principal place of business in this state shall notify the commissioner following the discovery of a breach in the security of any data processing system, including those of affiliates or subsidiaries as defined in R.S. 22:691.2, or the discovery or the receipt of notification of a breach in the security of a data processing system of a third-party service provider, including those of affiliates or subsidiaries as defined in R.S. 22:691.2, which contains the personal information or protected health information of any person regardless of whether or not data has actually been compromised.

C. Notification shall be made within ten days of the date of discovery of the breach, except as provided in Subsection D of this Section. The notification shall be provided electronically in the manner provided for on the department website and shall include the following information:

(1) The date of the incident.

(2) A description of the incident, including how the information was lost, stolen, or breached, and how the incident was discovered.

(3) The type of information lost, stolen, or breached.

(4) The period of time covered by the lost, stolen, or breached information.

(5) Whether the lost, stolen, or breached information has been recovered and, if so, how.

(6) Whether the information was encrypted or redacted and whether the encryption key was compromised.

(7) The number of Louisiana residents affected and the total number of people affected.

(8) A copy of any notification provided or intended to be provided to affected Louisiana residents and the date or anticipated date and method of notification.

(9) The identification of other regulatory or law enforcement agencies notified, if any, and the dates of notification.

(10) Whether a police report has been filed.

(11) Whether the individuals involved in the incident, both internal and external, have been identified.

(12) The results of any internal review identifying either a lapse in internal procedures or confirmation that all procedures were followed.

(13) The identification of remedial efforts being undertaken to cure the situation that permitted the breach to occur.

(14) Copies of the regulated person's privacy policies and data breach policies or procedures.

D. Each person required to provide notification pursuant to this Section shall submit a supplemental report to the notification at least every six months from the date of discovery of the breach and for no less than two years from the

date of discovery of the breach. Each supplemental report shall include any changes or updates to the information provided in the initial notification or the most recent supplemental report, as applicable. In addition, each person required to submit a supplemental report shall report once each year the total number of breaches experienced by the person and by any third-party service provider within the previous twelve months. The supplemental reports shall be made in the same manner as the initial notification.

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

F. Notification is not required if the personal information or protected health information involved is encrypted or redacted. The data shall not be considered to be encrypted if the encryption key has been acquired or compromised in the breach.

G. The commissioner may order specific corrective actions to be taken by any person required to provide notification pursuant to this Section, including but not limited to notifications to affected residents, the provision of credit monitoring services to affected residents, or the reporting of the breach to consumer credit agencies.

H. The commissioner may review the data breach policies, procedures, actions, and safeguards of any person required to provide notification pursuant to this Section, including but not limited to procedures to notify affected residents. The commissioner may order the institution of new policies and procedures where appropriate.

I. The commissioner may investigate and examine the records and operations of any person required to provide notification pursuant to this Section to determine if the person has implemented and complied with the orders issued pursuant to this Section.

J. Any person who fails to provide timely notifications, file supplemental reports as required by this Section, or comply with orders issued by the commissioner pursuant to this Section shall be subject, at the discretion of the commissioner, to either or both of the following:

(1) A fine not to exceed one thousand dollars for each violation, up to two million dollars in a calendar year, per person for all violations. Each day of noncompliance shall be deemed a separate violation.

(2) Suspension or revocation of the person's certificate of authority or license.

K. A person regulated by the department and affected by the commissioner's decisions, acts, or orders pursuant to this Section may demand a hearing in accordance with R.S. 22:2191 et seq.

L. The notifications to the commissioner and any supplemental reports required by this Section are exempt from disclosure pursuant to the Public Records Law and are hereby declared to be proprietary and confidential business records not subject to public examination or subpoena.

Section 2. R.S. 44:4.1(B)(11) is hereby amended and reenacted to read as follows:

§4.1 Exceptions

* * *

B. The legislature further recognizes that there exist exceptions, exemptions, and limitations to the laws pertaining to public records throughout the revised statutes and codes of this state. Therefore, the following exceptions, exemptions, and limitations are hereby continued in effect by incorporation into this Chapter by citation:

* * *

(11) R.S. 22:2, 14, 31, 42.1, **51,** 88, 244, 263, 265, 461, 550.7, 571, 572, 572.1, 574, 618, 639, 691.4, 691.5, 691.6, 691.7, 691.8, 691.9, 691.10, 732, 752, 753, 771, 834, 972(D), 1008, 1019.2, 1203, 1460, 1464, 1466, 1488, 1546, 1559, 1566(D), 1644, 1656, 1723, 1796, 1801, 1927, 1929, 1983, 1984, 2036, 2056, 2085, 2091, 2293, 2303

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

DIGEST

SB 103 Original 2016 Regular Session John Smith

Proposed law generally requires notification to the commissioner of certain data breaches. Provides for means and timing of notification and procedures therefor.

Proposed law provides for definition of terms, including data breach, encryption, personal and protected health information.

Proposed law provides that any person regulated by the department who owns or licenses computerized data shall notify the commissioner following the discovery of a breach in the security of any data processing system containing the personal information or protected health information of one or more residents of Louisiana, regardless of whether the data belonging to the Louisiana residents has actually been compromised.

Proposed law provides that any person regulated by the department shall notify the commissioner if the person discovers or is notified of a breach in the security of a data processing system of a third-party service provider that contains the personal information or protected health information of one or more residents of Louisiana, regardless of whether the data belonging to the Louisiana residents has actually been compromised.

Proposed law provides that any person regulated by the department and legally domiciled or having its principal place of business in this state shall notify the commissioner following the discovery of a breach in the security of any data processing system or the discovery or the receipt of notification of a breach in the security of a data processing system of a third-party service provider that contains the personal information or protected health information of any person regardless of whether or not the data has actually been compromised.

Proposed law provides that notification shall be made within 10 days of the date of discovery of the breach, except as provided in proposed law. Requires the notification to be provided electronically in the manner provided for on the department website and to include certain information; including date, description and duration of the incident, type of information compromised, and the number of Louisiana residents and total number of people affected.

Proposed law provides that a person required to provide notification shall submit a supplemental report to the notification at least every six months from the date of discovery of the breach and for no less than two years from the date of discovery of the breach. Provides that each supplemental report shall include any changes or updates to the information provided in the initial notification or the most recent supplemental report, as applicable. In addition, provides that the person shall report once each year the total number of breaches experienced by the person and by any third-party service provider within the previous 12 months.

Proposed law requires the notification to be 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. Provides that if a law enforcement agency determines that the notification to the commissioner required under proposed law would impede a criminal investigation, the notification may be delayed until the law enforcement agency determines that the notification will no longer compromise such investigation.

Proposed law provides that notification is not required if the personal information or protected health information involved is encrypted or redacted. Provides, however, that the data shall not be considered to be encrypted if the encryption key has been acquired in the breach.

Proposed law provides that the commissioner may order specific corrective actions to be taken by the person required to provide notification including but not limited to notifications to affected residents, the provision of credit monitoring services to affected residents, or the reporting of the breach to consumer credit agencies.

Proposed law provides that the commissioner may review the data breach policies, procedures, actions, and safeguards of the person required to provide notification including but not limited to procedures to notify affected residents. The commissioner may order the institution of new policies and procedures where appropriate.

Proposed law provides that the commissioner may investigate and examine the records and operations of any person required to provide notification to determine if the person has implemented and complied with the issued orders.

Proposed law provides that any person who fails to provide timely notifications, file supplemental reports, or comply with orders issued by the commissioner shall be subject, at the discretion of the commissioner, to either or both of the following:

(1) A fine not to exceed one thousand dollars for each violation, up to two million dollars in a calendar year, per person for all violations. Each day of noncompliance shall be deemed a separate violation.

(2) Suspension or revocation of the person's certificate of authority or license.

Proposed law provides that a person regulated by the department and affected by the commissioner's decisions, acts, or orders may demand a hearing in accordance with present law.

Proposed law provides that the notifications to the commissioner and any required supplemental reports shall be exempt from disclosure pursuant to the Public Records Law and are hereby declared to be proprietary and confidential business records not subject to public examination or subpoena.

Effective on August 1, 2016.

(Amends R.S. 44:4.1(B)(11); adds R.S. 22:51)