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

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

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

<u>Proposed law</u> 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.

<u>Proposed law</u> 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.

<u>Proposed law</u> 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.

<u>Proposed law</u> provides that notification shall be made within 10 days of the date of discovery of the breach, except as provided in <u>proposed law</u>. 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.

<u>Proposed law</u> 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.

<u>Proposed law</u> 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 <u>proposed law</u> 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.

<u>Proposed law</u> 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.

<u>Proposed law</u> 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.

<u>Proposed law</u> 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.

<u>Proposed law</u> 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.

<u>Proposed law</u> 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.

<u>Proposed law</u> 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 <u>present law</u>.

<u>Proposed law</u> 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)