GREEN SHEET REDIGEST

HB 614 **2020 Regular Session** **Seabaugh**

INSURANCE: Provides relative to data security for persons regulated by the commissioner of insurance

DIGEST

Proposed law enacts the Insurance Data Security Law to establish standards for data security and for the investigation of and notification to the commissioner of a cybersecurity event applicable to licensees of the Department of Insurance.

Proposed law defines "authorized individual", "consumer", "cybersecurity event", "encrypted", "information security program", "information system", "licensee", "multi-factor authentication", "nonpublic information", "person", "publicly available information", "risk assessment", and "third-party service provider".

Proposed law requires a licensee to develop, implement, and maintain a comprehensive, written information security program which satisfies the criteria required by proposed law and does all of the following:

(1) Protect the security and confidentiality of nonpublic information and the security of the information system.

(2) Protect against any threats or hazards to the security or integrity of nonpublic information and the information system.

(3) Protect against unauthorized access to or use of nonpublic information and minimize the likelihood of harm to any consumer.

(4) Define and periodically reevaluate a schedule for retention of nonpublic information and a mechanism for its destruction when no longer needed.

Proposed law requires a licensee to conduct a risk assessment that meets the criteria specified in proposed law, design an information security program to mitigate the identified risks, and implement appropriate security measures.

Proposed law provides for the duties of the licensee's board of directors.

Proposed law provides for the duties of a licensee with regard to third-party service providers.

Proposed law requires the licensee to monitor, evaluate, and adjust, as appropriate, the information security program consistent with any relevant changes in technology, the sensitivity of its nonpublic information, internal or external threats to information, and the licensee's own changing business arrangements.

Proposed law requires each licensee to establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event that compromises the confidentiality, integrity, or availability of nonpublic information in its possession, the licensee's information systems, or the continuing functionality of any aspect of the licensee's business or operations and establishes the minimum requirements of the response plan.

Proposed law requires a licensee which learns that a cybersecurity event has or may have occurred, or an outside vendor or service provider designated to act on behalf of the licensee, to conduct a prompt investigation and provides for the requirements of the investigation and subsequent documentation.

Proposed law provides for the notification duties of a licensee once there is a determination that a cybersecurity event has occurred.

Proposed law authorizes the commissioner to examine and investigate into the affairs of any licensee to determine whether the licensee has been or is engaged in any violation of proposed law and to take any action that is necessary or appropriate to enforce the provisions of proposed law whenever the commissioner has reason to believe that a licensee has been or is engaged in a violation of proposed law.

Proposed law provides for the confidentiality of any documents, materials, or other information in the control or possession of the commissioner that are furnished by a licensee or an employee or agent acting on behalf of a licensee pursuant to proposed law, including an exemption to the Public Records Law and prohibits the commissioner from making such information public.

Proposed law requiring a licensee to develop, implement, and maintain a comprehensive, written information security program does not apply to a licensee who meets any of the following criteria:

(1) Has fewer than 25 employees.

(2) Has less than $5 million in gross annual revenue.

(3) Has less than $10 million in year-end total assets.

(4) Establishes and maintains an information security program pursuant to the federal Health Insurance Portability and Accountability Act (HIPAA).

(5) Is an employee, agent, representative, or designee of a licensee, who is also a licensee, to the extent that the employee, agent, representative, or designee is covered by the information security program of the other licensee.

(6) Is affiliated with a depository institution subject to the Gramm-Leach-Bliley Act.

(7) Is subject to another jurisdiction approved by the commissioner.

Proposed law authorizes the commissioner to do any of the following in the event of a violation of proposed law:

(1) Suspend, revoke, or refuse to renew the certificate of authority or license of any insurer, person, or entity.

(2) Levy a fine not to exceed $1,000 for each violation per insurer, person, or entity, up to $100,000 aggregate for all violations in a calendar year per insurer, person, or entity.

(3) Order any insurer, person, or entity to cease and desist any action that violates any provision of proposed law.

Proposed law provides that the provisions of R.S. 22:2504(F) shall become effective on Aug. 1, 2022, the provisions of R.S. 22:250 shall become effective on Aug. 1, 2021, and Sections 1, 2, 3, and 4 shall become effective on Aug. 1, 2020.

(Amends R.S. 44:4.1(B)(11); adds R.S. 22:2501-2511)

Summary of Amendments Adopted by House

The Committee Amendments Proposed by House Committee on Insurance to the original bill:

1. Remove provision of proposed law which states the purpose and intent of proposed law and replace it with a provision which states that proposed law establishes exclusive standards for La. which are applicable to licensees for data security, the investigation of a cybersecurity event, and notification to the commissioner.

2. Specify that references in definitions of "cybersecurity event" and "information system" regarding information means nonpublic information.

3. Change a provision in the list of exclusions set forth in the definition of a "licensee" from a licensee acting as an assuming insurer that is domiciled in another state or jurisdiction to a person acting as such an assuming insurer.

4. Clarify that the definition of "nonpublic information" refers to electronic information.

5. Remove a provision of proposed law that defines "nonpublic information" as business-related information of a licensee that would cause an adverse impact to the business, operations, or security of the licensee if the information were to be tampered with or be disclosed, accessed, or used without authorization.

6. Clarify that the reference to an account number in the list of identifying information contained in the definition of "nonpublic information" is a financial account number.

7. Clarify that information or data created or derived from a healthcare provider or consumer be information that identifies a particular consumer in order for it to be identifying information for the purposes of defining "nonpublic information."

8. Add that a licensee who learns about a cybersecurity event relative to a third-party service provider's system make a reasonable effort to complete the steps required by proposed law or make a reasonable effort to confirm and document that the third-party service provider has completed such steps.

9. Change notice requirements from requiring that a licensee notify the commissioner of a cybersecurity event as promptly as possible but no later than seventy-two hours to requiring that a licensee furnish such notice without unreasonable delay but no later than three business days, and change subsequent notice requirement references of seventy-two hours to three business days.

10. Clarify that the notice requirement refers to a cybersecurity event involving nonpublic information in the possession of the licensee.

11. Add adjusters and public adjusters as defined in present law, R.S. 22:1661 and 1692, to the notification criterion regarding the licensee's domicile or home state.

12. Add to the criterion regarding the licensee's domicile or home state that the cybersecurity event has reasonable likelihood of materially harming either any consumer residing in this state or any material part of the normal operation of the licensee.

13. Clarify that subsequent notice requirements apply to material changes to previously provided information relative to the cybersecurity event.

14. Clarify that the requirements regarding what information be provided to the commissioner regarding the cybersecurity event be provided when making notice as required by proposed law.

15. Add an exception to the requirement that licensees give notice of a cybersecurity event when a system is maintained by a third-party service provider when the third-party service provider has already given notice as required by proposed law.

16. Add to the provision requiring notice when a cybersecurity event involves information accessed by the consumer through an independent insurance producer that such notice be required when it is required by the Database Security Breach Notification Law.

17. Change the requirement for when a cybersecurity event involves information accessed by the consumer through an independent insurance producer from as soon as practicable as directed by the commissioner to no later than the time at which notice is provided to the affected consumers.

18. Add to the provision requiring notice when a cybersecurity event involves information accessed by the consumer through an independent insurance producer that an insurer is excused from this obligation for any producers who are not authorized by law or contract to sell, solicit, or negotiate on behalf of the insurer.

19. Add to Public Records Law exception that the commissioner cannot otherwise make the documents, materials, or other information public.

20. Add a provision that excludes documents, materials, or other information in the control of the NAIC or a third-party from the Public Records Law.

21. Change the provision that a licensee is excluded from the information security program if the licensee has fewer than ten employees to if the licensee has fewer than twenty-five employees and remove the inclusion of independent contractors.

22. Add to the list of criteria for the exclusion of a licensee from the information security program that the licensee has less than five million dollars in gross annual revenue and less than ten million dollars in year-end total assets.

23. Add to the list of criteria for the exclusion of a licensee from the information security program if the licensee is subject to the Gramm-Leach-Bliley Act and meets the requirements of the act.

24. Add to the list of criteria for the exclusion of a licensee from the information security program if the licensee is subject to present law and notify affected consumers and the commissioner consistent with the requirements of the Gramm-Leach-Bliley Act.

25. Add that a licensee who satisfies the provisions of proposed law may assert a defense to any cause of action arising in tort and alleging the failure to implement reasonable information security controls resulted in a data breach of nonpublic information.

26. Add that the provisions of R.S. 22:2504(F) shall become effective on Aug. 1, 2022, the provisions of R.S. 22:250 shall become effective on Aug. 1, 2021, and Sections 1, 2, 3, and 4 shall become effective on Aug. 1, 2020.

Summary of Amendments Adopted by Senate

Committee Amendments Proposed by Senate Committee on Insurance to the reengrossed bill

1. Provides that a licensee subject to HIPAA who establishes and maintains a HIPAA-compliant information security program is required to submit a written statement certifying compliance only if requested by the commissioner in order to qualify as exempt from the proposed law information security program requirements.

2. Provides that a licensee affiliated with a depository institution subject to the Gramm-Leach-Bliley Act who establishes and maintains an information security program compliant with the requirements of that Act is required to submit a written statement certifying compliance only if requested by the commissioner in order to qualify as exempt from the proposed law information security program requirements.

3. Makes technical changes.