RÉSUMÉ DIGEST

ACT 283 (HB 614) **2020 Regular Session** **Seabaugh**

New 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.

New 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".

New law requires a licensee to develop, implement, and maintain a comprehensive, written information security program which satisfies the criteria required by new 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.

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

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

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

New 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.

New 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.

New 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.

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

New 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 new law and to take any action that is necessary or appropriate to enforce the provisions of new law whenever the commissioner has reason to believe that a licensee has been or is engaged in a violation of new law.

New 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 new law, including an exemption to the Public Records Law and prohibits the commissioner from making such information public.

New 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.

New law authorizes the commissioner to do any of the following in the event of a violation of new 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 new law.

New 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.

Effective Aug. 1, 2020.

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