TECHNICAL ADVISORY

TA 345 **July 29, 2020**

SUBJECT: 2020 Regular Session Act 283 HB 614 – Insurance Data Security Important New Requirements for ALL Insurance Licensees

BACKGROUND: The National Association of Insurance Commissioners (NAIC) developed the Insurance Data Security Model Law to establish data security standards for insurance licensees, provide for the investigation of cybersecurity events, and provide notification to the Commissioner of Insurance.

Eleven states have adopted some form of the model to date. Insurance Commissioner Jim Donelon introduced the model in the 2020 Regular Session of the Louisiana Legislature as HB 614, which has become law as Act 283.

IIABL had two very serious concerns with the original model and bill as introduced. One was the difficulty of compliance for small and medium size agencies. Second was the requirement that licensees ensure compliance by third-parties.

IIABL raised our concerns with Insurance Commissioner Jim Donelon. We want to thank Commissioner Donelon for working with us to amend HB 614 to exempt the great majority of agents from the difficult information security program implementation, and to modify the obligation to ensure compliance by third-parties.

Following is a summary of Act 283 to acquaint you with this new law.

It is important that all insurance licensees (including independent insurance agents) review their obligations under Act 283, which can be found HERE. Please refer to this statute for details.

Section 2509 Exemptions

For most independent agents, the section of Act 283 that they are going to be most interested in is Section 2509 Exemptions. There is an extensive list of exemptions outlined below. Licensees who meet ANY of these criteria are exempt from Section 2504, which is the requirement to maintain an extensive (and expensive) information security program. Please note that this does not mean that you have no obligation to safeguard your customers' personal information (you do have that obligation) but it means that you are not obligated to meet the extensive list of requirements for your information security program outlined in Section 2504.

Following are the exemptions from Section 2504 Information Security Program:

A. A licensee shall be exempt from the provisions of R.S. 22:2504 (requirement to maintain an information security program) if the licensee meets any of the following criteria:

(1) Having fewer than twenty-five employees.

(2) Less than five million dollars in gross annual revenue.

(3) Less than ten million dollars in year-end total assets.

(4) Being subject to the Health Insurance Portability and Accountability Act, Pub.L. 104-191, 110 Stat. 1936, and doing all of the following:
(a) Establishing and maintaining an information security program pursuant to any statutes, rules, regulations, procedures, or guidelines established pursuant to the Health Insurance Portability and Accountability Act.
(b) Complying with and submitting, upon request of the commissioner, a written statement certifying compliance with the information security program established and maintained pursuant to Subparagraph (a) of this Paragraph.

(5) Being 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) Being affiliated with a depository institution subject to the Interagency Guidelines Establishing Information Security Standards pursuant to the Gramm-Leach-Bliley Act, 15 U.S.C. 6801 and 6805, and doing all of the following:
(a) Establishing and maintaining an information security program pursuant to any statutes, rules, regulations, procedures, or guidelines established pursuant to the Gramm-Leach-Bliley Act.

(b) Complying with and submitting, upon request of the commissioner, a written statement certifying compliance with the information security program established and maintained pursuant to Subparagraph (a) of this Paragraph.

(7) Being subject to another jurisdiction approved by the commissioner and doing all of the following: (a) Establishing and maintaining an information security program pursuant to such statutes, rules, regulations, procedures, or guidelines established by another jurisdiction.
(b) Complying with and submitting a written statement certifying its compliance with the information security program established and maintained pursuant to Subparagraph (a) of this Paragraph.

Section 2504 Information Security Program

Licensees who are not exempt in Section 2509 must develop, implement, and maintain a comprehensive, written information security program which satisfies all of the criteria set out in Section 2504.

It is important to note that the information security program should be based on the licensee's risk assessment. Smaller licensees have a lower standard of care. The larger, more complex, and higher risk the licensee has…the more demanding the security program.

The list of criteria for the Information Security Program are five pages long. Too long to list here. If you are not exempt, please refer to Act 283, Section 2504.

For details on the requirement for the information security program, please refer to Act 283, Section 2504 which can be found HERE.

Section 2505 Investigation of a Cybersecurity Event

All licensees (no exemptions) are required to investigate any cybersecurity events including those of outside vendors or service providers that act on behalf of the licensee. The investigation must:

(1) Determine whether a cybersecurity event has occurred.

(2) Assess the nature and scope of the cybersecurity event.

(3) Identify any nonpublic information that may have been involved in the cybersecurity event.

(4) Undertake reasonable measures to restore the security of the information

(5) If a licensee learns that a cybersecurity event has or may have occurred in a system maintained by a third-party service provider, the licensee shall make reasonable efforts to confirm and document that the third-party service provider has completed these steps.

(6) The licensee shall maintain records concerning all cybersecurity events for a period of at least five years from the date of the cybersecurity event and shall produce those records upon demand of the commissioner

Section 2506 Notification of a Cybersecurity Event

A licensee shall notify the commissioner without unreasonable delay but in no event later than three business days from a determination that a cybersecurity event involving nonpublic information that is in the possession of the licensee has occurred when either of the following criteria has been met:

(1) Louisiana is the licensee's state of domicile and the cybersecurity event has reasonable likelihood of materially harming either of the following:

(a) Any consumer residing in this state.

(b) Any material part of the normal operations of the licensee.

(2) A licensee reasonably believes that the nonpublic information involved is for two hundred fifty or more consumers residing in Louisiana and that either of the following has occurred:

(a) A cybersecurity event affecting the licensee of which notice is required to be provided to any government body, self-regulatory agency, or any other supervisory body pursuant to any state or federal law.

(b) A cybersecurity event that has a reasonable likelihood of materially harming any of the following:

(i) Any consumer residing in this state.

(ii) Any material part of the normal operations of the licensee.

The licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the commissioner regarding material changes to previously provided information relative to the cybersecurity event.

The licensee making the notification required shall provide as much of the following information as possible in electronic form as directed by the

commissioner. There is a long list of information items specifically listed in the statute that must be reported.

A licensee shall comply with the Database Security Breach Notification Law, R.S. 51:3071 et seq., as applicable, and shall provide to the commissioner a copy of the notice sent to consumers if the licensee is required to notify the commissioner pursuant to the law.

In the case of a cybersecurity event in a system maintained by a third-party service provider of which the licensee has become aware, the licensee shall treat the cybersecurity event as if it were a breach of their own system, unless the third-party service provider gives the notice required.

For details on the reporting requirements for a cybersecurity event, please refer to Act 283, Section 2506 which can be found HERE.

Section 2507 Powers of the Commissioner

The commissioner may examine and investigate into the affairs of any licensee to determine whether the licensee has been or is engaged in any conduct in violation of this statute. This power is in addition to the normal powers which the Commissioner has under the law.

Whenever the commissioner has reason to believe that a licensee has been or is engaged in conduct in this state which violates this Chapter, the commissioner may take any action that is necessary or appropriate to enforce the provisions of this law.

Section 2508 Confidentiality

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 obtained by the commissioner in an investigation or examination shall be confidential by law and privileged, shall not be subject to release pursuant to the Public Records Law, shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action. However, the commissioner may use the documents, materials, or other information in the furtherance of any regulatory or legal action.

Neither the commissioner nor any person who received documents, materials, or other information while acting pursuant to the authority of the

commissioner shall testify in any private civil action concerning any confidential documents, materials, or information.

In order to assist in the performance of the commissioner's duties, the commissioner may share documents, materials, or other information with other state, federal, and international regulatory agencies, with the National Association of Insurance Commissioners (NAIC), and with state, federal, and international law enforcement authorities, if the recipient agrees in writing to maintain the confidentiality and privileged status of the document, material, or other information.

Section 2510 Penalties

In the case of a violation of this Chapter, the commissioner may impose a penalty pursuant to R.S. 22:18. (The normal insurance penalty statute.)

Section 2511 Defenses

A licensee that satisfies the provisions of this Chapter may assert an affirmative defense to any cause of action arising in tort that is brought pursuant to the laws of this state or in the courts of this state and that alleges that the failure to implement reasonable information security controls resulted in a data breach concerning nonpublic information.