Statement for the Record
From the National Association of Insurance Commissioners
for the U.S. House Financial Services Committee
Subcommittee on Financial Institutions and Consumer Credit
+HDULQJ RQ ³([DPLQLQJ WKH &XUUHQW 'DW5DH6 HFXULW\ 5HJL
February 14, 2018

Chairman Luetkemeyer, Ranking Member Clay, and members of the subcommittee, the National Association of Insurance Commissioners (NAIC)[1] appreciates the opportunity to submit this written statement for the hearing RQ ³Examining the Current Data Security and Breach Notification Regulatory Regime.´ State insurance regulators are keenly aware of the potentially devastating effects cyber-attacks can have on consumers and businesses and share your commitment to addressing cybersecurity risks and protecting consumer data. We recognize the importance of cybersecurity risk management and continue to work to further our efforts. All states have standards that comply with those set forth in the Gramm-Leach-

-

Bliley Act. Further, we recognize that with cybersecurity risks ... the protection of insurance consumer information ... the NAIC adopted the Insurance Data Security Model Law (attached) in October 2017. This model law updates state insurance regulatory requirements relating to data security, the investigation of a cyber event, and the notification ... state ... extensive input from ... cyber events ... regulated entities. The development of this model

and consumer representatives.

Specifically, the model ... requirements ... and other third-party service providers ... risk of

The model

...

2017 report on the asset management and insurance industries, the U.S Treasury Department endorsed the model and urged its prompt adoption.[2]

INSURANCE DATA SECURITY MODEL LAW

Table of Contents

Section 1. Title

This Act shall be known and may be cited as the “Insurance Data Security Law.”

Section 2. Purpose and Intent

A. The purpose and intent of this Act is to establish standards for data security and standards for the investigation of and notification to the Commissioner of a Cybersecurity Event applicable to Licensees, as defined in Section 3.

B. This Act may not be construed to create or imply a private cause of action for violation of its provisions nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.

Drafting Note:

The term “Cybersecurity Event” does not include the unauthorized acquisition of Encrypted Nonpublic Information if the en cryption, process or key is not also acquired, released or used without authorization.

Cybersecurity Event does not include an event with regard to which the Licensee has determined that the Nonpublic Information accessed by an unauthorized person has not been used or released and has been returned or destroyed.

E. “Department” means the [insert name of insurance regulatory body].

F. “Encrypted” means the transformation of data into a form which results in a low probability of assigning meaning without the use of a protective process or key.

G. “Information Security Program” means the administrative, technical, and physical safeguards that a Licensee uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle Nonpublic Information.

H. “Information System” means a discrete set of electronic information resources

a comprehensive written Information Security Program based on the Licensee's Risk Assessment and that contains administrative , technical, and physical safeguards for the protection of Nonpublic Information and the Licensee's Information System.

B. Objectives of Informat ion Security Program

A Licensee's Information Security Program shall be designed to:

(1) Protect the security and confidentiality of Nonpublic Information and the

edr;and t]TJ -1.1856 -1.2976 TD . Tc 0 Tw ( )Tj /.5928 -1.1036 TD .0015 Tc ((14)

T . DT 6792.10 02) (wT 0 cT75000. - DT 0 02BtOmks i

(1)

D. Risk Management

Based on its Risk Assessment, the Licensee shall:

(1)

(j) Implement measures to protect against destruction, loss, or damage of Nonpublic Information due to envi ronmental hazards, such as fire and water damage or other catastroph es or technological failures; and

(k) Develop, implement, and maintain procedures for the secure disposal of Nonpublic Information in any format.

(3) Include cybersecurity risks in the Lice nsee's enterprise risk management process.

(4) Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared; and

(5) Provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the Licensee in the Risk Assessment.

E. Oversight by Board of Directors

If the Licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum:

(1) Require the Licensee's executive management or its delegates to develop, implement, and maintain the Licensee's Information Security Program;

(2) Require the Licensee's executive management or its delegates to report in writing at least annually, the following information:

(a) The overall status of the Information Security Program and the Licensee's compliance with this Act; and

(b) Material matters related to the Information Security Program, addressing issues such as risk assessment, risk management and control decisions, Third-Party Service Provider arrangements, results of testing, Cybersecurity Events or violations and management's responses thereto, and recommendations for changes in the Information Security Program.

(3) If executive management delegates any of its responsibilities under Section 4 of this Act, it shall oversee the development, implementation and maintenance of the Licensee's Information Security Program prepared by the delegate(s) and shall receive a report from the delegate(s) complying with the requirements of the report to the Board of Directors above.

F. Oversight of Third-Party Service Provider Arrangements

(1) A Licensee shall exercise due diligence in selecting its Third-Party Service Provider; and

(2) A Licensee shall require a Third-Party Service Provider to implement appropriate administrative, technical, and physical measures to protect and

secure the Information Systems and Nonpublic Information that are accessible to, or held by, the Third-Party Service Provider.

G. Program Adjustments

The Licensee shall 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, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to Information Systems.

H. Incident Response Plan

(1) As part of its Information Security Program, each Licensee shall 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.

(2) Such incident response plan shall address the following areas:

(a) The internal process for responding to a Cybersecurity Event;

(b) The goals of the incident response plan;

(c) The definition of clear roles, responsibilities and levels of decision-making authority;

(d) External and internal communications and information sharing;

(e) Identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls;

(f) Documentation and reporting regarding Cybersecurity Events and related incident response activities; and

(g) The evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.

I. Annual Certification to Commissioner of Domiciliary State

Annually, each insurer domiciled in this State shall submit to the Commissioner, a written statement by February 15, certifying that the insurer is in compliance with the requirements set forth in Section 4 of this Act. Each insurer shall maintain for examination by the Department all records, schedules and data supporting this certificate for a period of five years. To the extent an insurer has identified areas, systems, or processes that require material improvement, updating or redesign, the insurer shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the Commissioner.

Insurance Data Security Model Law

(b) A Cybersecurity Event that has a reasonable likelihood of materially harming:

(i) Any Consumer residing in this State; or

(ii) Any material part of the normal operation(s) of the Licensee.

B. The Licensee shall provide as much of the following information as possible. The Licensee shall provide the information in electronic form as directed by the Commissioner. The Licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the Commissioner concerning the Cybersecurity Event.

(1) Date of the Cybersecurity Event;

(2) Description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of Third-Party Service Providers, if any;

(3) How the Cybersecurity Event was discovered;

(4) Whether any lost, stolen, or breached information has been recovered and if so, how this was done;

(5) The identity of the source of the Cybersecurity Event;

(6) Whether Licensee has filed a police re port or has notified any regulatory, government or law enforcement agencies and, if so, when such notification was provided;

(7) Description of the specific types of information acquired without authorization. Specific types of information means particular data elements including, for example, types of medical information, types of financial information or types of information allo wing identification of the Consumer;

(8) The period during which the Information System was compromised by the Cybersecurity Event;

(9) The number of total Consumers in this State affected by the Cybersecurity Event. The Licensee shall provide the best estimate in the initial report to the Commissioner and update this estimate with each subsequent report to the Commissioner pursuant to this section;

(10) The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed;

(11) Description of efforts being under taken to remediate the situation which permitted the Cybersecur ity Event to occur;

(12) A copy of the Licensee's privacy policy and a statement outlining the steps the Licensee will take to investigate and notify Consumers affected by the Cybersecurity Event; and

law] and any other notification requirements relating to a Cybersecurity Event imposed under Section 6.

F. Notice Regarding Cybersecurity Events of Insurers to Producers of Record

In the case of a Cybersecurity Event involving Nonpublic Information that is in the

(3) An employee, agent, representative or designee of a Licensee, who is also a