INSURANCE DATA SECURITY MODEL LAW

Table of Contents

tit.23, § 500, Cybersecurity Requirements for Financial Services Companies, effective March 1, 2017, such Licensee is also in [illegible]
with this Act.

Section 3. Definitions

As used in this Act, the following terms shall have these meanings:

A. "Authorized Individual" means an individual known to and screened by the Licensee and

D. “Cybersecurity Event” means an event resulting in unauthorized access to, disruption or misuse of, an Information System or information stored on such Information System.

The term “Cybersecurity Event” does not include the unauthorized acquisition of Encrypted Nonpublic Information if the encryption, 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

(a) Social Security number,

(b) Driver's license number or non-driver identification card number,

(c) Account number, credit or debit card number,

(d) Any security code, access code or password that would permit access to a Consumer's

(b) Information S

(h) Regularly test and monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, Information Systems;

(i) Include audit trails within the Information Security Program designed to detect and respond to Cybersecurity Events and designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Licensee;

(j) Implement measures to protect against destruction, loss, or damage of Nonpublic Information due to environmental hazards, such as fire and water damage or other catastrophes 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 Licensee'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

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

(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 undertaken to remediate the situation which permitted the Cybersecurity 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

(13) Name of a contact person who is both familiar with the Cybersecurity Event and authorized to act for the Licensee.

(2) (a) In the case of a Cybersecurity Event involving Nonpublic Information that is in the possession, custody or control of a Third-Party Service Provider of a Licensee that is an assuming insurer, the assuming insurer shall notify its affected ceding insurers and the Commissioner of its state of domicile within 72 hours of receiving notice from its Third-Party Service Provider that a Cybersecurity Event has occurred

(b) The ceding insurers that have a direct contractual relationship with affected Consumers shall fulfill the consumer notification requirements imposed under