INSURANCE DATA SECURITY MODEL LAW
Provisions Related to Third-Party Service Providers
[Proposed Revisions to Version 2 for Jan. 10 Drafting Group Call]

Section 3. Definitions

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

H. "Personal Information" means~~:~~ information possessed by a licensee or provided by a licensee to a third-party service provider and includes:

(1) A financial account number relating to a consumer, including a credit card number or debit card number, in combination with any security code, access code, password, or other personal identification information required to access the financial account; or

* * *

I. "Third-party service provider" means a person or entity, not otherwise defined as a licensee, that contracts with a licensee to maintain, process, store or otherwise have access to personal information under the licensee's possession, custody or control.

Section 4. Information Security Program

F. Oversight of Third-Party Service Provider Arrangements

The licensee shall:

(1) Exercise due diligence in selecting each third-party service provider; and

~~(1)~~(2) Confirm and document with each third-party service provider that it is able to implement appropriate measures to secure the licensee's personal information that is held in a system maintained by the third-party service provider.

~~contract only with third-party service providers that are capable of maintaining appropriate safeguards for personal information in the licensee's possession, custody or control, and the licensee shall be responsible for any failure by such third-party service providers to protect personal information provided by the licensee to the third-party service providers consistent with this Act.~~

Section 5. Investigation of a Data Breach

A. If the licensee learns that a data breach of personal information has or may have ~~occurred in relation to personal information in the possession, custody or control of the licensee or any of the licensee's third-party service providers, the~~occurred, the licensee, or a third party acting on behalf of that licensee, shall conduct a prompt investigation.

B. During the investigation, the licensee, or a third party acting on behalf of the licensee, shall, at a minimum:

(1) Assess the nature and scope of the data breach or potential data breach;

(2) Identify any personal information that may have been involved in the data breach;

(3) Determine whether the personal information has been acquired, released or used without authorization; and

(4) Perform or oversee reasonable measures to restore the security of the information systems compromised in the data breach in order to prevent further unauthorized acquisition, release or use of personal information in the licensee's possession, custody or control.

C. If the licensee learns that a data breach has or may have occurred in in a system maintained by a third-party service provider, the licensee will confirm and document that the third-party service provider has completed the steps listed in Section 5B above.

Section 6. Notification of a Data Breach

A. If following an investigation under Section 5, the licensee determines that an unauthorized acquisition of personal information listed in Section 3H(1), (2)(a) through (f), (3) or (4) involved in a data breach has occurred, the licensee, or a third party acting on behalf of the licensee, shall notify:

* * *

B. Notification to the Commissioner

Notwithstanding the responsibilities prescribed in Sections 5A and 6A of this Act, no later than three (3) business days after determining that a data breach has occurred, the licensee, or a third party acting on behalf of the licensee, shall notify the commissioner that a data breach has occurred. The licensee shall provide as much of the following information as possible:

*** * ***

C. Notification to Consumer Reporting Agencies

The licensee, or a third party acting on behalf of the licensee, shall notify, as expediently as possible and without unreasonable delay, after determining that a data breach has occurred, each consumer reporting agency, if the data breach involves personal information listed in Section 3H(1), (2)(a) through (f), (3) or (4) relating to 500 or more consumers. Notification must include the date of the data breach, an estimate of the number of persons affected by the data breach, if known, and the actual or anticipated date that persons were or will be notified of the data breach.

D. Notification to Consumers

The licensee, or a third party acting on behalf of the licensee, shall notify all consumers whose personal information listed in Section 3H(1), (2)(a) through (f), (3) or (4) was affected as expediently as possible and without unreasonable delay, and in no case later than sixty (60) calendar days after determining that a data breach has occurred.

*** * ***

E. Notice Regarding Data Breaches of Third-Party Service Providers

In the event of a data breach in a system maintained by a third-party service provider, the licensee shall comply with the notice requirements of Sections 6A through D., unless the third-party service provider has agreed to send the notices. In the event that the third-party service provider agrees to send the notices, licensee will confirm and document that this was completed. The computation of licensee's deadlines shall begin on the day after the third-party service provider notifies the licensee of the data breach or the licensee otherwise has actual knowledge of the data breach, whichever is sooner.

F. Notice Regarding Data Breaches of Insurers to Reinsurers

(1) In the event of a data breach involving personal information listed in Section 3H(1), (2)(a) through (f), (3) or (4) where the licensee is acting as an assuming insurer and does not have a direct contractual relationship with the affected consumers:

(a) The assuming insurer shall notify its affected ceding insurers and the Commissioner of its state of domicile; and

(b) The ceding insurers that have a direct contractual relationship with the affected consumers shall fulfill the notification requirements imposed under Section 6A through D.

(2) In the event of a data breach involving personal information listed in Section 3H(1), (2)(a) through (f), (3) or (4) that is held in a system maintained by a third-party service provider of a licensee acting as an assuming insurer and does not have a direct contractual relationship with the affected consumers, the third-party service provider shall notify the licensee of the data breach immediately upon determination that a breach has occurred.

G. Notice Regarding Data Breaches of Insurers to Producers of Record

In the event of a data breach involving personal information listed in Section 3H(1), (2)(a) through (f), (3) or (4) where the licensee is an insurer, the insurer shall, without unreasonable delay, notify the producers of record of all affected consumers.