Revisions noted in yellow from the industry trade association draft.
Revisions noted in gray are additional revisions proposed by IIABA and NAIFA.

Section 3. Definitions

P. "Third-Party Service Provider" means a Person, not otherwise defined as a Licensee, that contracts with a Licensee licensed in this or any other state to maintain, process, store or otherwise is permitted access to Nonpublic Information through its provision of services to the Licensee.

Section 5. Investigation of a Cybersecurity Event

A. If the Licensee learns that a Cybersecurity Event has or may have occurred the Licensee, or an outside vendor and/or service provider designated to act on behalf of the Licensee, shall conduct a prompt investigation.

B. During the investigation, the Licensee, or an outside vendor and/or service provider designated to act on behalf of the Licensee, shall, at a minimum determine as much of the following information as possible:

(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; and

(4) Perform or oversee reasonable measures to restore the security of the Information Systems compromised in the Cybersecurity Event in order to prevent further unauthorized acquisition, release or use of Nonpublic Information in the Licensee's possession, custody or control.

~~C. If the Licensee learns that a Cybersecurity Event has or may have occurred in a system maintained by a Third-Party Service Provider, the Licensee will complete the steps listed in Section 5B above or confirm and document that the Third-Party Service Provider has completed those steps.~~

D. 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 9. Exceptions

A. The following exceptions shall apply to this Act:

(1) A Licensee meeting any of the following criteria is exempt from Section 4 of this Act~~:~~:

(a) Fewer than ~~ten~~ 25 [*or insert other number*] employees~~, including any independent contractors~~, or

(b) Less than $5 million in gross annual revenue, or

(c) Less than $10 million in year-end total assets.

(2) A Licensee subject to Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996 (Health Insurance Portability and Accountability Act) that has established and maintains an Information Security Program pursuant to such statutes, rules, regulations, procedures or guidelines established thereunder, will be considered to meet the requirements of Section 4, provided that Licensee is compliant with~~, and submits a written statement certifying its compliance with,~~ the same;

(3) An employee, agent, representative or designee of a Licensee, who is also a Licensee, is exempt from this Act ~~Section 4 and need not develop its own Information Security Program~~ to the extent that the employee, agent, representative or designee is covered by the Information Security Program of the other Licensee.

B. In the event that a Licensee ceases to qualify for an exception, such Licensee shall have 180 days to comply with this Act.