National Association of Insurance Commissioners' ("NAIC") Final *Insurance Data Security Model Law* (v.6) v. New York State Department of Financial Services' ("NYSDFS") Final *Cybersecurity Requirements for Financial Services Companies*

This chart compares the *final* NAIC's Insurance Data Security Model Law (v.6)[1] and the *final* NYSDFS' Cybersecurity Requirements for Financial Services Companies. Significantly, in the final version of the Model Law the NAIC included a drafting note stating: **if a Licensee is in compliance with the NYSDFS regulation, it shall also be in compliance with the Act** (Section 2).[2] Version 6 also expands the exclusions of those who are not "Licensees" to include "a Licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction," in addition to "a purchasing group or a risk retention group chartered and licensed in a state other than this State" (Section 3(I)). The NAIC further removed the "best practices" condition, which was a part of the information security requirements for the Licensee's Information Security Program (Section 4(D)(2)). Licensees may now determine which security measures are "appropriate" to implement, rather than being obligated to use the "best practices" for cybersecurity protection for an entity of their size and complexity. There were also substantial changes to the provisions regarding oversight of Third-Party Service Provider (TPSP) arrangements. Now, a Licensee must exercise "due diligence" in selecting its TPSP and must require a TPSP to implement appropriate measures to protect and secure the Information Systems and Nonpublic Information that are accessible to, or held by, the TPSP (Section 4(F)). In earlier iterations of the Model Law, Licensees would have been required to complete risk assessments of the TPSP. Version 6 also requires annual, written certification by February 15 to the Commissioner certifying that the insurer is in compliance with the Act (Section 4(I)). In previous versions, the certification only would have been required upon the Commissioner's request, and the filing date would have been up to the Commissioner's discretion. The NAIC also changed the timeframe to notify producers of record of all affected Consumers of a Cybersecurity Event—to "as soon as practicable as directed by the Commissioner" (rather than within 72 hours of a Cybersecurity Event as initially proposed) (Section 6(F)).

Other notable changes include:

- Clarifying that notification to the Commissioner of a Cybersecurity Event is required when certain listed criteria has been met (Section 6(A)).
- Permitting the Commissioner to share confidential documents with a third-party consultant or vendor provided that the consultant agrees to keep the documents confidential and privileged (Section 8(C)(3)).
- Allowing a Licensee subject to the Health Insurance Portability and Accountability Act that has an Information and Security Program pursuant to the Act to be deemed to have met the requirements of Section 4, provided that the Licensee is actually compliant with (and submits a statement certifying its compliance with) the same (Section 9(A)(2)

[1] Edits/additions to Version 6 of the NAIC data security model law are highlighted in red, major deletions indicated with ~~strikethrough~~.

[2] The drafting note reads: "The drafters of this Act intend that if a Licensee, as defined in Section 3, is in compliance with N.Y. Comp. Codes R. & Regs. tit.23, § 500, Cybersecurity Requirements for Financial Services Companies, effective March 1, 2017, such Licensee is also in compliance with this Act" (Section 2).

	NAIC Final Insurance Data Security Model Law (v.6)	NYSDFS Final Cybersecurity Requirements for Financial Services Companies
Definitions **Cyber Event**	**Section 3. Definitions** *Cybersecurity Event* means any 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 determined that the Nonpublic Information accessed by an unauthorized person has not been used or released and has been returned or destroyed.	**Section 500.01 Definitions.** *Cybersecurity Event* means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.
Technology Terms	*Information System* means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems. *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. *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.	*Information System* means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

	Multi-Factor Authentication means authentication through verification of at least two of the following types of authentication factors: (1) Knowledge factors, such as a password; or (2) Possession factors, such as a token or text message on a mobile phone; or (3) Inherence factors, such as a biometric characteristic. *Risk Assessment* means the Risk Assessment that each Licensee is required to conduct under Section 4C of this Act.	*Multi-Factor Authentication* means authentication through verification of at least two of the following types of authentication factors: (1) Knowledge factors, such as a password; or (2) Possession factors, such as a token or text message on a mobile phone; or (3) Inherence factors, such as a biometric characteristic. *Penetration Testing* means a test methodology in which assessors attempt to circumvent or defeat the security features of an Information System by attempting penetration of databases or controls from outside or inside the Covered Entity's Information Systems. *Risk Assessment* means the risk assessment that each Covered Entity is required to conduct under section 500.09 of this Part. *Risk-Based Authentication* means any risk-based system of authentication that detects anomalies or changes in the normal use patterns of a Person and requires additional verification of the Person's identity when such deviations or changes are detected, such as through the use of challenge questions.
Definitions (cont.) **Personal Information** **&** **Public Information**	*Nonpublic Information* means information that is not Publicly Available Information and is: (1) Business related information of a Licensee the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Licensee; (2) Any information concerning a Consumer which because of name, number, personal mark, or other identifier can be used to identify such Consumer, in combination with any one or more of the following data elements: (a) Social Security number,	*Nonpublic Information* shall mean all electronic information that is not Publicly Available Information and is: (1) Business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity; (2) Any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) 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 financial account, or (e) Biometric records; (3) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or a Consumer and that relates to (a) The past, present or future physical, mental or behavioral health or condition of any Consumer or a member of the Consumer's family, (b) The provision of health care to any Consumer, or (c) Payment for the provision of health care to any Consumer. *Publicly Available Information* means any information that a Licensee has a reasonable basis to believe is lawfully made available to the general public from: federal, state or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state or local law. For the purposes of this definition, a Licensee has a reasonable basis to believe that information is lawfully made available to the general public if the Licensee has taken steps to determine: (1) That the information is of the type that is available to the general public; and (2) Whether a Consumer can direct that the information not be made available to the general public and, if so, that such Consumer has not done so.	(ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records; (3) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual. *Publicly Available Information* means any information that a Covered Entity has a reasonable basis to believe is lawfully made available to the general public from: federal, state or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state or local law. (1) For the purposes of this subsection, a Covered Entity has a reasonable basis to believe that information is lawfully made available to the general public if the Covered Entity has taken steps to determine: (i) That the information is of the type that is available to the general public; and (ii) Whether an individual can direct that the information not be made available to the general public and, if so, that such individual has not done so.

Definitions (Cont.) **Relevant Entities, Stakeholders, Etc.**	**Section 3. Definitions** *Consumer* means an individual, including but not limited to applicants, policyholders, insureds, beneficiaries, claimants, and certificate holders who is a resident of this State and whose Nonpublic Information is in a Licensee's possession, custody or control. *Department* means the [insert name of insurance regulatory body]. *Authorized Individual* means an individual known to and screened by the Licensee and determined to be necessary and appropriate to have access to the Nonpublic Information held by the Licensee and its Information Systems. *Licensee* means any Person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this State but shall not include a purchasing group or a risk retention group chartered and licensed in a state other than this State or a Licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction. *Person* means any individual or any non-governmental entity, including but not limited to any nongovernmental partnership, corporation, branch, agency or association.	**Section 500.01 Definitions.** *Affiliate* means any Person that controls, is controlled by or is under common control with another Person. For purposes of this subsection, control means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of stock of such Person or otherwise. *Authorized User* means any employee, contractor, agent or other Person that participates in the business operations of a Covered Entity and is authorized to access and use any Information Systems and data of the Covered Entity. *Covered Entity* means any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law. *Person* means any individual or non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency or association. *Senior Officer(s)* means the senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, information systems, compliance and/or risk of a Covered Entity, including a branch or agency of a foreign banking organization subject to this Part.

	Third-Party Service Provider means a Person, not otherwise defined as a Licensee, that contracts with a Licensee to maintain, process, store or otherwise is permitted access to Nonpublic Information through its provision of services to the Licensee.	*Third Party Service Provider*(s) means a Person that (i) is not an Affiliate of the Covered Entity, (ii) provides services to the Covered Entity, and (iii) maintains, processes or otherwise is permitted access to Nonpublic Information through its provision of services to the Covered Entity.
Information Security or Cybersecurity Program **Objectives of Information Security or Cyber Program**	**Section 4. Information Security Program** *A. Implementation of an Information Security Program* Commensurate with the size and complexity of the Licensee, the nature and scope of the Licensee's activities, including its use of Third-Party Service Providers, and the sensitivity of the Nonpublic Information used by the Licensee or in the Licensee's possession, custody or control, each Licensee shall develop, implement, and maintain 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 Information Security Program* A Licensee's Information Security Program shall be designed to: (1) Protect the security and confidentiality of Nonpublic Information and the security of the Information System; (2) Protect against any threats or hazards to the security or integrity of Nonpublic Information and the Information System; (3) Protect against unauthorized access to or use of Nonpublic Information, and minimize the likelihood of harm to any Consumer; and (4) Define and periodically reevaluate a schedule for retention of Nonpublic Information and a mechanism for its destruction when no longer needed.	**Section 500.02 Cybersecurity Program.** (a) *Cybersecurity Program*. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. (b) The cybersecurity program shall be based on the Covered Entity's **Risk Assessment** and designed to perform the following core cybersecurity functions: (1) identify and assess internal and external cybersecurity risks that may threaten the security or integrity of Nonpublic Information stored on the Covered Entity's Information Systems. (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts; (3) detect Cybersecurity Events; (4) respond to identified or detected Cybersecurity Events to mitigate any negative effects; (5) recover from Cybersecurity Events and restore normal operations and services; and (6) fulfill all regulatory reporting obligations. (c) A Covered Entity may meet the requirement(s) of this Part by adopting the relevant and applicable provisions of a cybersecurity program maintained by an Affiliate, provided that such provisions

		satisfy the requirements of this Part, as applicable to the Covered Entity. (d) All documentation and information relevant to the Covered Entity's cybersecurity program shall be made available to the superintendent upon request. **Section 500.04 Chief Information Security Officer.** (a) Chief Information Security Officer. Each Covered Entity shall designate a qualified individual responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy (for purposes of this Part, "Chief Information Security Officer" or "CISO"). The CISO may be employed by the Covered Entity, one of its Affiliates or a Third Party Service Provider To the extent this requirement is met using a Third Party Service Provider or an Affiliate the Covered Entity shall: (1) retain responsibility for compliance with this Part; (2) designate a senior member of the Covered Entity's personnel responsible for direction and oversight of the Third Party Service Provider; and (3) require the Third Party Service Provider to maintain a cybersecurity program that protects the Covered Entity in accordance with the requirements of this Part.
Oversight and Assessing Risk	*C. Risk Assessment* The Licensee shall: (1) Designate one or more employees, an affiliate, or an outside vendor designated to act on behalf of the Licensee who is responsible for the Information Security Program; (2) Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission,	**Section 500.09 Risk Assessment.** Each Covered Entity shall conduct a periodic Risk Assessment of the Covered Entity's Information Systems sufficient to inform the design of the cybersecurity program as required by this Part. Such Risk Assessment shall be updated as reasonably necessary to address changes to the Covered Entity's Information Systems, Nonpublic Information or business operations. The Covered Entity's Risk Assessment shall allow for revision of controls to respond to

	disclosure, misuse, alteration or destruction of Nonpublic Information, including the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third-Party Service Providers; (3) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Nonpublic Information; (4) Assess the sufficiency of policies, procedures, Information Systems and other safeguards in place to manage these threats, including consideration of threats in each relevant area of the Licensee's operations, including: (a) **Employee training and management**; (b) Information Systems, including network and software design, as well as information classification, governance, processing, storage, transmission, and disposal; and (c) Detecting, preventing, and responding to attacks, intrusions, or other systems failures; and (5) Implement information safeguards to manage the threats identified in its ongoing assessment, and no less than annually assess the effectiveness of the safeguards' key controls, systems, and procedures. A summary of this assessment shall be included in the annual report required by Section 4I.	technological developments and evolving threats and shall consider the particular risks of Covered Entity's business operations related to cybersecurity, Nonpublic Information collected or stored, Information Systems utilized and the availability and effectiveness of controls to protect Nonpublic Information and Information Systems. (a) The Risk Assessment shall be carried out in accordance with written policies and procedures and shall be documented. Such policies and procedures shall include: (1) criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the Covered Entity; (2) criteria for the assessment of the confidentiality, integrity, security and availability of the Covered Entity's Information Systems and Nonpublic Information, including the adequacy of existing controls in the context of identified risks; and (3) requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the cybersecurity program will address the risks.
Access Limitations	*<u>D. Risk Management</u>* Based on its Risk Assessment, the Licensee shall: (1) Design its Information Security Program to mitigate the identified risks, commensurate with the size and complexity of the Licensee's activities, including its use of Third-Party Service Providers, and the sensitivity of the Nonpublic Information used by the Licensee or in the Licensee's possession, custody or control.	**Section 500.07 Access Privileges.** As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.

Employee Training (NAIC- *see* Sec. 4(C)(4)(a) *above*)	(2)Determine which security measures listed below are appropriate to implement. ~~In making this determination, the Licensee shall use the best practices for cybersecurity protection, detection, and remediation available commensurate with the size and complexity of the Licensee's activities, including its use of Third-Party Service Providers, and the sensitivity of the Nonpublic Information used by the Licensee or in the Licensee's possession, custody or control.~~ (a) Place **access controls** on Information Systems, including controls to authenticate and permit access only to Authorized Individuals to protect against the unauthorized acquisition of Nonpublic Information;	**Section 500.14 Training and Monitoring.** *(See also 500.10)* As part of its cybersecurity program, each Covered Entity shall: (a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users; and (b) provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the identified by the Covered Entity in its Risk Assessment.
Minimum requirements for Information Security or Cyber Program	(b) Identify and manage data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with their relative importance to business objectives and the organization's risk strategy; (c) Restrict access at physical locations containing Nonpublic Information, only to authorized individuals; (d) Protect by encryption or other appropriate means, all Nonpublic Information while being transmitted over an external network and all Nonpublic Information stored on a laptop computer or other portable computing or storage device or media; (e) Adopt secure development practices for in-house developed applications utilized by the Licensee and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Licensee; (f) Modify the Information System in accordance with the Licensee's Information Security Program; (g) Utilize effective controls, which may include multi-factor	**Section 500.03 Cybersecurity Policy.** *Cybersecurity Policy*. Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board or directors (or appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address the following areas to the extent applicable to the Covered Entity's operations: (a) information security; (b) data governance and classification; (c) asset inventory and device management; (d) **access controls** and identity management; (*See also Section 500.07)* (e) business continuity and disaster recovery planning and resources; (f) systems operations and availability concerns; (g) systems and network security; (h) systems and network monitoring; (i) systems and application development and quality assurance; (j) physical security and environmental controls; (k) customer data privacy; (l) vendor and Third-Party Service Provider management;

System Testing	authentication procedures for any individual accessing Nonpublic Information. (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 (5) Provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the Licensee in the Risk Assessment.	(m) risk assessment; and (n) incident response *(see below).* **Section 500.05 Penetration Testing and Vulnerability Assessments.** The cybersecurity program for each Covered Entity shall include monitoring and testing, developed in accordance with the Covered Entity's Risk Assessment, designed to assess effectiveness of cybersecurity program. The monitoring and testing shall include continuous monitoring or periodic Penetration Testing and vulnerability assessments. Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, Covered Entities shall conduct: (a) annual **Testing** of the Covered Entity's Information Systems determined each given year based on relevant identified risks in accordance with the Risk Assessment; and (b) bi-annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the Covered Entity's Information Systems based on the Risk Assessment.

Response Procedures	*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.	**Section 500.03(a)(n)** incident response. **Section 500.16 Incident Response Plan.** (a) As part of its cybersecurity program, each Covered Entity shall establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event materially affecting the confidentiality, integrity or availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business or operations. (b) Such incident response plan shall address the following areas: (1) the internal processes for responding to a Cybersecurity Event; (2) the goals of the incident response plan; (3) the definition of clear roles, responsibilities and levels of decision-making authority; (4) external and internal communications and information sharing; (5) identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls; (6) documentation and reporting regarding Cybersecurity Events and related incident response activities; and (7) the evaluation and revision of the incident response plan following a Cybersecurity Event.
Board Oversight	*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	*(See Section 500.03 Cybersecurity Policy listed above and 500.4 below)*

	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.	
Report Requirements	*I. Annual ~~Report~~ 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. ~~Upon the Commissioner's request, and no more than once each~~	**Section 500.04 Chief Information Security Officer.** (b) **Report**. The CISO of each Covered Entity shall report in writing at least annually to the Covered Entity's board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a Senior Officer of the Covered Entity responsible for the Covered Entity's cybersecurity program. The CISO shall **report** on the Covered Entity's cybersecurity program and material cybersecurity risks. The report shall consider to the extent applicable: (1) the confidentiality of Nonpublic Information and the integrity and security of the Covered Entity's Information Systems; (2) the Covered Entity's cybersecurity policies and procedures; (3) material cybersecurity risks to the Covered Entity; (4) overall effectiveness of the Covered Entity's cybersecurity program; and

Third-Party Service Providers	~~year, each insurer domiciled in this State shall file an annual written report with the Commissioner. The report, which may reference or incorporate other filings with any other state, federal, and international regulatory agencies, shall summarize the assessment mandated by Subsection 4C(5) above and any areas, systems or processes that require material improvement, updating or redesign. The insurer shall document the remedial efforts planned and underway to address such areas, systems or processes. Such documentation shall be available for inspection by the Commissioner.~~ ~~[Drafting Note: In order to ensure that the Commissioner is receiving the most current information from an insurer, Section 4I recognizes that the time for filing the Annual Report during the calendar year may vary from insurer to insurer, depending on the timing of the insurer's assessment. In any event, the report shall be filed once each year, with the insurer apprising the Commissioner as to the anticipated time of filing.]~~ *F. Oversight of Third-Party Service Provider* ["TPSP"] *Arrangements* (1) A Licensee shall exercise due diligence in selecting its TPSP; and (2) A Licensee shall require a TPSP 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 TPSP. ~~Each Licensee shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, TPSPs. Such policies and procedures shall be based on the Risk Assessment of the Licensee and shall address to the extent applicable:~~ ~~(a) The identification and risk assessment of TPSPs;~~	(5) material Cybersecurity Events involving the Covered Entity during the time period addressed by the report. *(See Sections 500.03(l) and 500.04(a) listed above)* **Section 500.11 Third Party Service Provider Security Policy.** (a) Third Party Information Security Policy. Each Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, TPSPs. Such policies and procedures shall be based on the Risk Assessment of the Covered Entity and shall address to the extent applicable: (1) the identification and risk assessment of TPSPs; (2) minimum cybersecurity practices required to be met by such TPSPs in order for them to do business with the Covered Entity; (3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such TPSPs; and (4) periodic assessment of such TPSPs s based on the risk they present and the continued adequacy of their cybersecurity practices. (b) Such policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to TPSPs including to the extent applicable guidelines addressing: (1) the TPSP's policies and procedures for access controls, including its use of Multi-Factor Authentication as required by section 500.12 of this Part, to limit access to relevant Information Systems and Nonpublic Information; (2) the TPSP's policies and procedures for the use of encryption as required by section 500.15 of this Part to protect Nonpublic Information in transit and at rest; (3) notice to be provided to the Covered Entity in the event of a Cybersecurity Event directly impacting the Covered Entity's

	~~(b) Minimum cybersecurity practices required to be met by such TPSPs in order for them to do business with the Licensee;~~ ~~(c) Due diligence processes used to evaluate the adequacy of cybersecurity practices of such TPSPs; and~~ ~~(d) Periodic assessment of such TPSPs based on the risk they present and the continued adequacy of their cybersecurity practices.~~ ~~(2) Such policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to TPSPs including, to the extent applicable, guidelines addressing:~~ ~~(a) The TPSP's policies and procedures for access controls, including its use of Multi-Factor Authentication, to limit access to relevant Information Systems and Nonpublic Information;~~ ~~(b) The TPSP's policies and procedures for use of Encryption to protect Nonpublic Information in transit and at rest;~~ ~~(c) Notice to be provided to the Licensee in the event of a Cybersecurity Event directly impacting the Licensee's Information Systems or Nonpublic Information being held by the TPSP; and~~ ~~(d) Representations and warranties addressing the TPSP's cybersecurity policies and procedures that relate to the security of the Licensee's Information Systems or Nonpublic Information.~~ *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	information systems or the Covered Entity's Nonpublic Information being held by the TPSP; and (4) representations and warranties addressing the TPSP's cybersecurity policies and procedures that relate to the security of the Covered Entity's Information Systems or Nonpublic Information. (c) Limited Exception. An agent, employee, representative or designee of a Covered Entity who is itself a Covered Entity need not develop its own Third Party Information Security Policy pursuant to this section if the agent, employee, representative or designee follows the policy of the Covered Entity that is required to comply with this Part.

	arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to Information Systems.	
Other Security Requirements **Data Audits**	*See* Section 4(D)(2)(i): (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;	**Section 500.06 Audit Trail.** (a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity (b) Each Covered Entity shall maintain records required by section 500.06(a)(1) of this Part for not fewer than five years and shall maintain records required by section 500.06(a)(2) of this Part for not fewer than three years.
Application Security	*See* above Section 4(D)(2)(e): (e) Adopt secure development practices for in-house developed applications utilized by the Licensee and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Licensee;	**Section 500.08 Application Security.** (a) Each Covered Entity's cybersecurity program shall include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the Covered Entity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Covered Entity within the context of the Covered Entity's technology environment. (b) All such procedures, guidelines and standards shall be periodically reviewed, assessed and updated as necessary by the CISO (or a qualified designee) of the Covered Entity.
Cyber Personnel and Training	*See* Section 4(C)(4)(a)	**Section 500.10 Cybersecurity Personnel and Intelligence.** (a) Cybersecurity Personnel and Intelligence. In addition to the requirements set forth in section 500.04(a) of this Part, each Covered Entity shall: (1) utilize qualified cybersecurity personnel of the Covered Entity, an Affiliate or a Third Party Service Provider sufficient to manage the

		Covered Entity's cybersecurity risks and to perform or oversee the performance of the core cybersecurity functions specified in section 500.02(b)(1)-(6) of this Part; (2) provide cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks; and (3) verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures. (b) A Covered Entity may choose to utilize an Affiliate or qualified Third Party Service Provider to assist in complying with the requirements set forth in this Part, subject to the requirements set forth in section 500.11 of this Part.
Multi-Factor Authentication	*See* general requirements relating to "authenticating" access in Section 4(D)(2)(g).	**Section 500.12 Multi-Factor Authentication.** (a) Multi-Factor Authentication. Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems. (b) Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls.
Limits on Data Retention	*See* reference to "disposal" of information, Section 4(D)(2)(k): (k) Develop, implement, and maintain procedures for the secure disposal of Nonpublic Information in any format	**Section 500.13 Limitations on Data Retention.** As part of its cybersecurity program, each Covered Entity shall include policies and procedures for the secure disposal on a periodic basis of any Nonpublic Information identified in section 500.01(g)(2)-(3) of this Part that is no longer necessary for business operations or for other legitimate business purposes of the Covered Entity, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

Encryption	*See* Section 4(D)(2)(d): (d) Protect by encryption or other appropriate means, all Nonpublic Information while being transmitted over an external network and all Nonpublic Information stored on a laptop computer or other portable computing or storage device or media;	**Section 500.15 Encryption of Nonpublic Information.** (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. (1) To the extent a Covered Entity determines that encryption of Nonpublic Information in transit over external networks is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO. (2) To the extent a Covered Entity determines that encryption of Nonpublic Information at rest is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.
Investigation of Cybersecurity Event	**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; (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.	No similar provision.

	C. If the Licensee learns that a Cybersecurity Event has or may have occurred in a system maintained by a TPSP, the Licensee will complete the steps listed in Section 5B above or confirm and document that the TPSP 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.	
Cybersecurity Event Notification **Commissioner Notification**	**Section 6. Notification of a Cybersecurity Event** *A. Notification to the Commissioner* Each Licensee shall notify the Commissioner as promptly as possible but in **no event later than 72 hours** from a determination that a Cybersecurity Event has occurred ~~if~~ when either of the following criteria has been met: (1) This State is the Licensee's state of domicile, in the case of an insurer, or this State is the Licensee's home state, in the case of a producer, as those terms are defined in [insert reference to Producer Licensing Model Act]; or (2) The Licensee reasonably believes that the Nonpublic Information involved is of 250 or more Consumers residing in this state and that is either of the following: (a) A Cybersecurity Event impacting 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; or (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	No similar provision. **Section 500.17 Notices to Superintendent.** (a) Notice of Cybersecurity Event. Each Covered Entity shall notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred that is either of the following: (1) Cybersecurity Events impacting the Covered Entity of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or (2) Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity. (b) **Annually** each Covered Entity shall submit to the superintendent a written statement covering the prior calendar year. This statement shall be submitted by February 15 in such form set forth as Appendix A, certifying that the Covered Entity is in compliance with the requirements set forth in this Part. Each Covered Entity shall maintain for examination by the Department all records, schedules and data supporting this certificate for a period of five years. To the extent a Covered Entity has identified areas, systems or processes that require material improvement, updating or redesign, the Covered Entity 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 superintendent.

Notification (Cont.)	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 TPSPs, 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 report 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 allowing 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 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.	
Consumer Notification	<u>*C. Notification to Consumers*</u>. Licensee shall comply with [insert state's data breach notification law], as applicable, and provide a copy of the notice sent to Consumers under that statute to the Commissioner, when a Licensee is required to notify the Commissioner under Section 6A.[3]	No similar provision.
Third-Party Breach Notification	<u>*D. Notice Regarding Cybersecurity Events of Third-Party Service Providers*</u> (1) In the case of a Cybersecurity Event in a system maintained by a TPSP, of which the Licensee has become aware ~~received notice~~, the Licensee shall treat such event as it would under Section 6A. (2) The computation of Licensee's deadlines shall begin on the day after the TPSP notifies the Licensee of the Cybersecurity Event or the Licensee otherwise has actual knowledge of the Cybersecurity Event, whichever is sooner. (3) Nothing in this Act shall prevent or abrogate an agreement between a Licensee and another Licensee, a TPSP or any other party to fulfill any of the investigation requirements imposed under Section 5 or notice requirements imposed under Section 6.	No similar provision.
	<u>*E. Notice Regarding Cybersecurity Events of Reinsurers to*</u>	No similar provision.

[3] **NB**: NAIC model law V.4 **<u>removed</u>** the requirements to notify credit reporting agencies and substantially lessened the consumer notification requirements.

Reinsurer Notification	*Insurers* (1) (a) In the case of a Cybersecurity Event involving Nonpublic Information that is used by the Licensee that is acting as an assuming insurer or in the possession, custody or control of a Licensee that is acting as an assuming insurer and that does not have a direct contractual relationship with the affected Consumers, the assuming insurer shall notify its affected ceding insurers and the Commissioner of its state of domicile **within 72 hours** of making the determination 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 [insert the state's breach notification law] and any other notification requirements relating to a Cybersecurity Event imposed under Section 6. (2) (a) In the case of a Cybersecurity Event involving Nonpublic Information that is in the possession, custody or control of a TPSP 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 TPSP** 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 [insert the state's breach notification 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 possession, custody or control of a Licensee that is an insurer or its TPSP and for which a Consumer accessed the insurer's services through an	No similar provision.

	independent insurance producer, the insurer shall notify the producers of record of all affected Consumers **as soon as practicable as directed by the Commissioner** ~~**within 72 hours of making the determination that a Cybersecurity Event has occurred.**~~ The insurer is excused from this obligation for those instances in which it does not have the current producer of record information for any individual Consumer.	
Consumer Protections Post-Breach	**[REMOVED** from earlier versions provisions re: identify theft protection**]**	No similar provision.
Enforcement	**Section 7. Power of Commissioner** A. The commissioner shall have power to 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 Act. This power is in addition to the powers which the commissioner has under [insert applicable statutes governing the investigation or examination of insurers]. Any such investigation or examination shall be conducted pursuant to [insert applicable statutes governing the investigation or examination of insurers]. B. Whenever the Commissioner has reason to believe that a Licensee has been or is engaged in conduct in this state which violates this Act, the Commissioner may take action that is necessary or appropriate to enforce the provisions of this Act.	**Section 500.20 Enforcement.** This regulation will be enforced by the superintendent pursuant to, and is not intended to limit, the superintendent's authority under any applicable laws.
Exemptions / Exceptions	**Section 9. Exceptions** A. The following exceptions shall apply to this Act: (1) A Licensee with fewer than ten employees, including any independent contractors is exempt from Section 4 [re: Information Security Program] of this Act; (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, ~~or~~	**Section 500.19 Exemptions.** (a) Limited Exemption. Each Covered Entity with: (1) fewer than 10 employees, including any independent contractors, of the Covered Entity or its Affiliates, or (2) less than $5,000,000 in gross annual revenue in each of the last three fiscal years from New York business operations of the Covered Entity and its Affiliates, and (3) less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including

	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 ~~can produce, upon request, documentation satisfactory to the Commissioner that independently validates such compliance~~; (3) An employee, agent, representative or designee of a Licensee, who is also a Licensee, is exempt from 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.	assets of all Affiliates, shall be exempt from the requirements of sections 500.04, 500.05, 500.06, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part. (b) An employee, agent, representative or designee of Covered Entity, who is itself a Covered Entity, is exempt from this Part and need not develop its own cybersecurity program to the extent that the employee, agent, representative or designee is covered by the cybersecurity program of the Covered Entity. (c) A Covered Entity that does not directly or indirectly operate, maintain, utilize or control any Information Systems, and that does not, and is not required to, directly or indirectly control, own, access, generate, receive or possess Nonpublic Information shall be exempt from the requirements of sections 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part. (d) A Covered Entity under Article 70 of the Insurance Law that does not and is not required to directly or indirectly control, own, access, generate, receive or possess Nonpublic Information other than information relating to its corporate parent company (or Affiliates) shall be exempt from the requirements of sections 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part. (e) A Covered Entity that qualifies for any of the above exemptions pursuant to this section shall file a Notice of Exemption in the form set forth as Appendix B within 30 days of the determination that the Covered Entity is exempt. (f) The following Persons are exempt from the requirements of this Part, provided such Persons do not otherwise qualify as a Covered Entity for purposes of this Part: Persons subject to Insurance Law section 1110; Persons subject to Insurance Law section 5904; and any accredited reinsurer or certified reinsurer that has been accredited or

		certified pursuant to 11 NYCRR 125. (g) In the event that a Covered Entity, as of its most recent fiscal year end, ceases to qualify for an exemption, such Covered Entity shall have 180 days from such fiscal year end to comply with all applicable requirements of this Part.
Certification	*Section 4(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.	**Section 500.21 Effective Date.** This Part will be effective March 1, 2017. Covered Entities will be required to annually prepare and submit to the superintendent a Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations under Section 500.17(b) of this Part commencing February 15, 2018.
Penalties	**Section 10. Penalties** In the case of a violation of this Act, a Licensee may be penalized in accordance with [insert general penalty statute].	No similar provision.
Confidentiality	**Section 8. Confidentiality** A. Any documents, materials or other information in the control or possession of the Department that are furnished by a Licensee or an employee or agent thereof acting on behalf of Licensee pursuant to Section 4I, Section 6B(2), (3), (4), (5), (8), (10), and (11), or that are obtained by the Commissioner in an investigation or examination pursuant to Section 7 of this Act shall be confidential by law and privileged, shall not be subject to [insert reference to state open records, freedom of information, sunshine or other appropriate law], shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action. However,	**Section 500.18. Confidentiality** Information provided by a Covered Entity pursuant to this Part is subject to exemptions from disclosure under the Banking Law, Insurance Law, Financial Services Law, Public Officers Law or any other applicable state or federal law.

	the Commissioner is authorized to use the documents, materials or other information in the furtherance of any regulatory or legal action brought as a part of the Commissioner's duties. B. Neither the Commissioner nor any person who received documents, materials or other information while acting under the authority of the Commissioner shall be permitted or required to testify in any private civil action concerning any confidential documents, materials, or information subject to Section 8A. C. In order to assist in the performance of the Commissioner's duties under this Act, the commissioner: (1) May share documents, materials or other information, including the confidential and privileged documents, materials or information subject to Section 8A, with other state, federal, and international regulatory agencies, with the NAIC, its affiliates or subsidiaries, and with state, federal, and international law enforcement authorities, provided that the recipient agrees in writing to maintain the confidentiality and privileged status of the document, material or other information; (2) May receive documents, materials or information, including otherwise confidential and privileged documents, materials or information, from the NAIC, its affiliates or subsidiaries and from regulatory and law enforcement officials of other foreign or domestic jurisdictions, and shall maintain as confidential or privileged any document, material or information received with notice or the understanding that it is confidential or privileged under the laws of the jurisdiction that is the source of the document, material or information; and (3) May share documents, materials or other information subject to Section 8A, with a third-party consultant or vendor provided the consultant agrees in writing to maintain the	

	confidentiality and privileged status of the document, material or other information. (4) May enter into agreements governing sharing and use of information consistent with this subsection. D. No waiver of any applicable privilege or claim of confidentiality in the documents, materials, or information shall occur as a result of disclosure to the commissioner under this section or as a result of sharing as authorized in Section 8C. E. Nothing in this Act shall prohibit the insurance commissioner from releasing final, adjudicated actions that are open to public inspection pursuant to [insert appropriate reference to state law] to a database or other clearinghouse service maintained by the NAIC, its affiliates or subsidiaries. [Drafting Note: States conducting an investigation or examination under their examination law may apply the confidentiality protections of that law to such an investigation or examination.]	
Other	**Section 11. Rules and Regulations [OPTIONAL]** The Commissioner may, in accordance with [the state statute setting forth the ability of the Department to adopt regulations] issue such regulations as shall be necessary to carry out the provisions of this Act. [Drafting Note: This provision is applicable only to states requiring this language.] **Section 13. Effective Date** This Act shall take effect on [insert a date]. Licensees shall have **one year** from the effective date of this Act to implement Section 4 of this Act and two years from the effective date of this Act to implement Section 4(F) of this Act.	No similar provision.