Scott A. Sinder
202 429 6289
ssinder@steptoe.com

1330 Connecticut Avenue, NW
Washington, DC 20036-1795
202 429 3000 main
www.steptoe.com

Steptoe
STEPTOE & JOHNSON LLP

May 22, 2018

TO: The Council of Insurance Agents & Brokers

FROM: Scott Sinder
Josh Oppenheimer

RE: **South Carolina Insurance Data Security Act**

On May 3, 2018, South Carolina Governor Henry McMaster signed into law the South Carolina Insurance Data Security Act (the "South Carolina Act").[1] The South Carolina Act puts into place a robust privacy/cyber security regime and with its enactment South Carolina is the first state to implement the National Association of Insurance Commissioners' ("NAIC") Insurance Data Security Model Law (#668) ("NAIC Model Law").[2]

The South Carolina Act closely tracks the NAIC Model Law with only two notable exceptions. First, the South Carolina Act exempts communications service provider, specifically stating: "Nothing in this chapter creates any duty or liability for a provider of communication services for the transmission of voice, data, or other information over its network" (Section 38-99-100).

---

[1] 2018 S.C. ACTS 171, *available at* https://www.scstatehouse.gov/sess122_2017-2018/bills/4655.htm. Once codified into the South Carolina Code of Laws, the Act will appear in Title 38, Chapter 99.

[2] Insurance Data Security Model Law (MDL-668), *available at* http://www.naic.org/store/free/MDL-668.pdf.

Second, the South Carolina law provides for shorter implementation periods than those contemplated by the NAIC Model Act. The South Carolina Act provides a January 1, 2019 effective date for the Act itself; a July 1, 2019 effective date for the requisite Information Security Program; and a July 1, 2020 for the required Oversight of Third-Party Service Provider Arrangements.

The South Carolina Act also closely tracks the NYSDFS Rule in many respects. For example, major definitions are aligned, along with several of the major cybersecurity/data security program requirements (e.g., Oversight of Third-Party Service Providers). In fact, in many instances, the language is identical. The South Carolina Act also incorporates technical requirements, such as application security (Sec. 38-99-20(D)(2)(e)) and audit trails (Sec. 38-99-20(D)(2)(i)), as well as an incident response provision (Sec. 38-99-20(H)) and exemptions to the Act (Sec. 38-99-70), which mimic the requirements in the NYSDFS Rule.

The biggest difference between the South Carolina Act and the NYSDFS Rule relates to notification requirements. The South Carolina Act contains several provisions requiring to consumer and law enforcement notification, while the NYSDFS Rule only requires notifying the New York Superintendent of Financial Services in the event of breach. In addition, while many of the data security/cyber program requirements are similar, the NYSDFS regulations generally contain more stringent and specific technology requirements (e.g., NYSDFS has specific technology requirements for web applications).

The attached chart summarizes the South Carolina Act requirements and notes the few deviations from the NAIC Model Law.[3] The chart also compares the South Carolina Act with the New York State Department of Financial Services' ("NYSDFS") Cybersecurity Requirements for Financial Services Companies ("NYSDFS Rule").[4]

[3] Material edits/additions between the South Carolina Act and the NAIC Model Law are highlighted in red, and major deletions are indicated with ~~strikethrough~~.

[4] New York Department of Financial Services, Final Rule, Cybersecurity Requirements for Financial Services Companies, 23 NYCRR 500 (Feb. 16, 2017), *available at* https://www.dfs.ny.gov/legal/regulations/adoptions/rf23-nycrr-500_cybersecurity.pdf.

South Carolina Insurance Data Security Act v. New York State Department of Financial Services' ("NYSDFS") Final Rule
Cybersecurity Requirements for Financial Services Companies

	South Carolina Insurance Data Security Act	NYSDFS Final Cybersecurity Requirements for Financial Services Companies
Definitions	**Section 38-99-10.**	**Section 500.01 Definitions.**
Cyber Event	<u>*Cybersecurity Event*</u> means an event resulting in unauthorized access to or the disruption or misuse of an information system or information stored on an 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. The term 'cybersecurity event' also 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.	<u>*Cybersecurity Event*</u> 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	<u>*Information System*</u> 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 or process controls systems, telephone switching and private branch exchange systems, and environmental control systems. <u>*Information Security Program*</u> 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. <u>*Encrypted*</u> means the transformation of data into a form which	<u>*Information System*</u> 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.

	results in a low probability of assigning meaning without the use of a protective process or key. *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 this chapter.	*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**	*Nonpublic Information* means information that is not publicly available information and is: (a) 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; (b) any information concerning a consumer which because of name, number, personal mark, or other identifier can be used to	*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

Information	identify such consumer, in combination with any one or more of the following data elements: (i) social security number; (ii) driver's license number or nondriver identification card number; (iii) account number, credit or debit card number; (iv) security code, access code, or password that would permit access to a consumer'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 a consumer and that relates to: (i) the past, present or future physical, mental or behavioral health or condition of a consumer or a member of the consumer's family; (ii) the provision of health care to a consumer; or (iii) payment for the provision of health care to a consumer. <u>*Publicly Available Information*</u> means information that a licensee has a reasonable basis to believe is lawfully made available to the general public from federal, state, or local governmental 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 item, a licensee has a reasonable basis to believe information is lawfully made available to the general public if the licensee has taken steps to determine: (a) that the information is of the type that is available to the general public; and (b) whether a consumer can direct that the information not be made available to the general public and, if so, that the	individual, in combination with any one or more of the following data elements: (i) Social Security number, (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. <u>*Publicly Available Information*</u> 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

	consumer has not done so.	done so.
Definitions (Cont.) **Relevant Entities, Stakeholders, Etc.**	*Consumer* means an individual including, but not limited to, an applicant, policyholder, insured, beneficiary, claimant, and certificate holder who is a resident of this State and whose nonpublic information is in a licensee's possession, custody, or control. *Department* means the Department of Insurance. *Authorized Individual* means an individual known to and screened by the licensee and determined to be necessary and appropriate to have access to nonpublic information held by the licensee and its information systems. *Licensee* means a person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this State but does 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 nongovernmental entity including, but not limited to, a nongovernmental partnership, corporation, branch, agency, or association. *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.	*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*(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 38-99-20.** (A) 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) A licensee's information security program must be designed to: (1) protect the security and confidentiality of nonpublic information and the security of the information system; (2) protect against 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 a 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) The Licensee shall: (1) designate one or more employees, an affiliate, or an outside vendor designated to act on behalf of the licensee as responsible for the information security program; (2) identify reasonably foreseeable internal or external threats that could result in the unauthorized access to or transmission, disclosure, misuse, alteration, or destruction of nonpublic information including the security of information systems and	**Section 500.09 Risk Assessment.** (a) 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 technological developments and evolving threats and shall consider

	nonpublic information that are accessible to or held by third party service providers; (3) assess the likelihood and potential damage of these threats, considering the sensitivity of the nonpublic information; (4) assess the sufficiency of policies, procedures, information systems, and other safeguards in place to manage these threats, taking into consideration threats in each relevant area of the licensee's operations, including: (a) **employee training and management**; (b) information systems, including network and software design, and 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 at least 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.~~ *[The South Carolina Act does not contain this cross-reference to the annual report.]*	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. (b) 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	(D) 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 (SC Act – *see* above Sec. 38-99-20(C)(4)(a))	(2) determine the appropriateness of and implement the following security measures: (a) placing **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; (b) identifying and managing the 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;	**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	(c) restricting access at physical locations containing nonpublic information to authorized individuals; (d) protecting 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) adopting secure development practices for in house developed applications used by the licensee and procedures for evaluating, assessing, ~~or~~ and testing the security of externally developed applications used by the licensee; (f) modifying the information system in accordance with the licensee's information security program; (g) utilizing effective controls, which may include multifactor authentication procedures for an individual accessing nonpublic information; (h) **regularly testing and monitoring systems** and procedures to detect actual and attempted attacks on, or intrusions into,	**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;

System Testing	information systems; (i) including **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) implementing 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) developing, implementing, and maintaining 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 use 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.	(l) vendor and Third-Party Service Provider management; (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) (1) As part of its information security program, a licensee must establish a written incident response plan designed to promptly respond to, and recover from, a 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.	**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

	(2) An incident response plan required in item (1) must address: (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.	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) (1) If the licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum: (a) require the licensee's executive management or its delegates to develop, implement, and maintain the licensee's information security program; (b) require the licensee's executive management or its delegates to **report** in writing at least annually: (i) the overall status of the information security program and the licensee's compliance with this chapter; and (ii) material matters related to the information security program addressing issues such as risk assessment, risk management and control decisions, third party service provider arrangements, testing results, cybersecurity events or violations and management's responses, and recommendations for changes in the information security program. (2) If the executive management of a licensee delegates any of	*[See Section 500.03 Cybersecurity Policy listed above and 500.4 below]*

	its responsibilities under this chapter, it shall oversee the development, implementation, and maintenance of the licensee's information security program prepared by the delegates and receive a report from the delegates which must comply with the requirements of the report to the board of directors.	
Report Requirements	(I) Annually, each insurer domiciled in this State shall submit to the director, a written statement by February fifteenth, certifying that the insurer is in compliance with the requirements set forth in this section. 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 director.	**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 (5) material Cybersecurity Events involving the Covered Entity during the time period addressed by the report.
Third-Party Service Providers	(F) A licensee shall: (1) exercise due diligence in selecting its third party service provider; and (2) 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	*[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:

	service provider. (G) The licensee shall monitor, evaluate and adjust 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 including, but not limited to, mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.	(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 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.
Other Security Requirements **Data Audits**	*See* above Section 38-99-20(D)(2)(i): (i) including **audit trails** within the information security program designed to detect and respond to cybersecurity events and designed to reconstruct material financial transactions	**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 the licensee;	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 38-99-20(D)(2)(e): (e) adopting secure development practices for in house developed applications used by the licensee and procedures for evaluating, assessing, ~~or~~ and testing the security of externally developed applications used 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* above Section 38-99-20(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 "authentication" access in Section 38-99-20(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 38-99-20(D)(2)(k):	**Section 500.13 Limitations on Data Retention.** As part of its cybersecurity program, each Covered Entity shall

Encryption	(k) developing, implementing, and maintaining procedures for the secure disposal of nonpublic information in any format; *See* above Section 38-99-20(D)(2)(d): (d) protecting 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;	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. **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. (b) To the extent that a Covered Entity is utilizing compensating controls under (a) above, the feasibility of encryption and effectiveness of the compensating controls shall be reviewed by the CISO at least annually.
Investigation of Cybersecurity Event	**Section 38-99-30.** (A) If a licensee learns that a cybersecurity event has occurred or may have occurred, the licensee, an outside vendor, or	No similar provision.

	service provider designated to act on behalf of the licensee must conduct a prompt investigation of the event. (B) During the investigation, the licensee, outside vendor, or service provider designated to act on behalf of the licensee shall, at a minimum: (1) determine whether a cybersecurity event occurred; (2) assess the nature and scope of the cybersecurity event; (3) identify 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 occurred or may have occurred in a system maintained by a third party service provider, the licensee shall complete an investigation pursuant to the requirements of this section or confirm and document that the third party service provider has completed an investigation pursuant to the requirements of this section. 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 produce those records upon demand of the director.	
Cybersecurity Event Notification **Commissioner Notification**	**Section 38-99-40.** (A) A licensee shall notify the director ~~as promptly as possible but in no event~~ no later than seventy two hours after determining that a cybersecurity event has occurred when either of the following criteria are met: (1) South Carolina is the licensee's state of domicile in the case	No similar provision. **Section 500.17 Notices to Superintendent.**

Notification (Cont.)	of an insurer, or the licensee's home state in the case of a producer; or (2) the licensee reasonably believes that the nonpublic information involved is of no less than two hundred and fifty consumers residing in this State, and the cybersecurity event: (a) impacts the licensee of which notice is required to be provided to any governmental body, self regulatory agency, or any other supervisory body pursuant to state or federal law; or (b) has a reasonable likelihood of materially harming a consumer residing in this State or a material part of the normal operations 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 director. The licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the director concerning the cybersecurity event. The information sent to the director must include: (1) the date of the cybersecurity event; (2) a 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 the licensee has filed a police report or has notified any regulatory, governmental or law enforcement agencies and, if so, when such notification was provided; (7) a description of the specific types of information acquired without authorization, which means particular data elements including, for example, types of medical information, types of financial information, or types of information allowing	(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.

	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, in which case the licensee shall provide the best estimate in the initial report to the director and update this estimate with each subsequent report to the director 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) a 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) the name of a contact person who is both familiar with the cybersecurity event and authorized to act on behalf of the licensee.	
Consumer Notification	(C) A licensee shall comply with the notice requirements of Section 39-1-90, and other applicable law and provide a copy of the notice sent to consumers to the director when a licensee is required to notify the director.	No similar provision.
Third-Party Breach	(D) (1) In the case of a cybersecurity event in a system maintained by a third party service provider of which the	No similar provision.

Notification	licensee has become aware, the licensee shall treat such event as it would under subsection (A) (2) The computation of the licensee's deadlines shall begin on the day after the third party service provider 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 chapter shall prevent or abrogate an agreement between a licensee and another licensee, a third party service provider or any other party to fulfill any of the investigation requirements or notice requirements imposed under this chapter	
Reinsurer Notification	(E)(1)(a) In the case of a cybersecurity event involving nonpublic information used by the licensee who is acting as an assuming insurer or in the possession, custody, or control of a licensee who 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 director of its state of domicile **within seventy two hours** of making the determination that a cybersecurity event has occurred. (b) A ceding insurer that has a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under Section 39-1-90, and other notification requirements relating to a cybersecurity event imposed under this chapter. (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 who is an assuming insurer, the assuming insurer shall notify its affected ceding insurers and the director of its state of domicile **within seventy two hours after receiving notice from its third party service**	No similar provision.

	provider that a cybersecurity event has occurred. (b) A ceding insurer that has a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements of Section 39-1-90, and other notification requirements relating to a cybersecurity event imposed under this chapter. (F) 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 third party service provider and for which a consumer accessed the insurer's services through an independent insurance producer, the insurer shall notify the producers of record of all affected consumers **as soon as practicable** as directed by the director. The insurer is excused from this obligation for those instances in which it does not have the current producer of record information for an individual consumer.	No similar provision.
Enforcement	**Section 38-99-50.** (A) The director has the power and authority to examine and investigate into the affairs of a licensee to determine whether the licensee ~~has been or~~ is engaged in conduct in violation of this chapter. This power is in addition to the powers which the director has under this title. An investigation or examination must be conducted pursuant to Section 38-13-10, et seq. (B) When the director has reason to believe that a licensee is engaged in conduct in this State which violates the provisions of this chapter, the director may take necessary and appropriate action to enforce the provisions of this chapter.	**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	**Section 38-99-70.** (A) The following licensees are exempt from the provisions of this chapter: (1) a licensee with fewer than ten employees, including any	**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

	independent contractors ~~is exempt from Section 4 [Information Security Program] of this Act~~; (2) an employee, agent, representative or designee of a licensee, who is also a licensee, is exempt from the provisions of this chapter 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; and (3) a licensee subject to the **Health Insurance Portability and Accountability Act**, Pub.L. 104-191, 110 Stat. 1936, 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 this chapter, provided that the licensee is compliant with, and submits a written statement certifying its compliance with, the provisions of this chapter. (B) In the event that a licensee ceases to qualify for an exception, such licensee shall **have one hundred and eighty days** to comply with this chapter.	(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 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	**Time Effective, Section 6.** This act takes effect January 1, 2019. *See* above Section 38-99-20(I): Annually, each insurer domiciled in this State shall submit to the director, a written statement by February fifteenth, certifying that the insurer is in compliance with the requirements set forth in this section. 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 director.	**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 38-99-80.** A licensee who violates a provision of this chapter is subject to penalties as provided in Section 38-2-10.	No similar provision.

Confidentiality	**Section 38-99-60.** (A) Documents, materials, or other information in the control or possession of the department that are furnished by a licensee or an employee or agent acting on behalf of a licensee, or obtained by the director in an investigation or examination are confidential by law and privileged, are not subject to disclosure under the Freedom of Information Act, and are not subject to subpoena or discovery in a private or civil action; and are not admissible as evidence in a private or civil action. However, the director is authorized to use the documents, materials, or other information in the furtherance of a regulatory or legal action brought as a part of the director's duties. (B) The director or a person who received documents, materials, or other information while acting under the authority of the director may not be permitted or required to testify in a private civil action concerning confidential documents, materials, or information. (C) To assist in the performance of his duties, the director may: (1) share documents, materials, or other information, including confidential and privileged documents, materials, or information, with other state, federal, and international regulatory agencies the National Association of Insurance Commissioners, its affiliates or subsidiaries, and state, federal, and international law enforcement authorities, provided that the recipient agrees in writing to maintain the confidentiality and privileged status of the documents, materials, or other information; (2) receive documents, materials, or information, including otherwise confidential and privileged documents, materials, or information, from the National Association of Insurance Commissioners, its affiliates or subsidiaries and from regulatory and law enforcement officials of other foreign or domestic jurisdictions, and maintain as confidential or	**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.

	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; (3) share documents, materials, or other information 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; and (4) enter into an agreement governing the 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 may occur from disclosure to the director under this section or sharing as authorized under this chapter. (E) Nothing in this chapter prohibits the director from releasing final, adjudicated actions that are open to public inspection to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners, its affiliates, or subsidiaries.	
Other	**Section 38-99-90.** The director is authorized to promulgate regulations necessary for the administration of this chapter. **Section 38-99-100.** Nothing in this chapter creates any duty or liability for a provider of communication services for the transmission of voice, data, or other information over its network. *[The Model Law does not contain this provision.]* **Delayed Implementation Date, Section 4**	No similar provision. No similar provision. **Section 500.22 Transitional Periods.**

	Licensees have until **July 1, 2019**, to implement Section 38-99-20 of this act and until **July 1, 2020**, to implement Section 38-99-20(F) of this act. *[The Model Law provides delayed implementation dates that are one and two years from the effective date. The South Carolina Act's delayed implementation dates are six and 18 months from the effective date.]*	(a) Transitional Period. Covered Entities shall have 180 days from the effective date of this Part to comply with the requirements set forth in this Part, except as otherwise specified. (b) The following provisions shall include additional transitional periods. Covered Entities shall have: (1) One year from the effective date of this Part to comply with the requirements of sections 500.04(b), 500.05, 500.09, 500.12, and 500.14(b) of this Part. (2) Eighteen months from the effective date of this Part to comply with the requirements of sections 500.06, 500.08, 500.13, 500.14 (a) and 500.15 of this Part. (3) Two years from the effective date of this Part to comply with the requirements of section 500.11 of this Part.
	Severability, Section 5. If any section, subsection, paragraph, subparagraph, sentence, clause, phrase, or word of this act is for any reason held to be unconstitutional or invalid, such holding shall not affect the constitutionality or validity of the remaining portions of this act, the General Assembly hereby declaring that it would have passed this act, and each and every section, subsection, paragraph, subparagraph, sentence, clause, phrase, and word thereof, irrespective of the fact that any one or more other sections, subsections, paragraphs, subparagraphs, sentences, clauses, phrases, or words hereof may be declared to be unconstitutional, invalid, or otherwise ineffective.	**Section 500.23 Severability.** If any provision of this Part or the application thereof to any Person or circumstance is adjudged invalid by a court of competent jurisdiction, such judgment shall not affect or impair the validity of the other provisions of this Part or the application thereof to other Persons or circumstances.