South Carolina General Assembly
122nd Session, 2017-2018

S. 856

STATUS INFORMATION

General Bill
Sponsors: Senator Cromer
Document Path: l:\council\bills\nbd\11180cz18.docx

Introduced in the Senate on January 9, 2018
Currently residing in the Senate Committee on **Banking and Insurance**

Summary: SC Insurance Data Security Act

HISTORY OF LEGISLATIVE ACTIONS

Date	Body	Action Description with journal page number
1/9/2018	Senate	Introduced and read first time (Senate Journal-page 81)
1/9/2018	Senate	Referred to Committee on **Banking and Insurance** (Senate Journal-page 81)

View the latest legislative information at the website

VERSIONS OF THIS BILL

1/9/2018

A BILL

TO AMEND THE CODE OF LAWS OF SOUTH CAROLINA, 1976, TO ENACT THE "SOUTH CAROLINA INSURANCE DATA SECURITY ACT" BY ADDING CHAPTER 99 TO TITLE 38 SO AS TO DEFINE NECESSARY TERMS; TO REQUIRE A LICENSEE TO DEVELOP, IMPLEMENT AND MAINTAIN A COMPREHENSIVE INFORMATION SECURITY PROGRAM BASED ON THE LICENSEE'S RISK ASSESSMENT AND TO ESTABLISH CERTAIN REQUIREMENTS FOR THE SECURITY PROGRAM, TO PROVIDE MINIMUM REQUIREMENTS FOR A LICENSEE'S BOARD OF DIRECTORS, IF APPLICABLE, TO REQUIRE A LICENSEE TO MONITOR THE SECURITY PROGRAM AND MAKE ADJUSTMENTS IF NECESSARY, TO PROVIDE THAT THE LICENSEE MUST ESTABLISH AN INCIDENT RESPONSE PLAN AND TO ESTABLISH CERTAIN REQUIREMENTS FOR THE INCIDENT RESPONSE PLAN, TO REQUIRE A LICENSEE TO SUBMIT A STATEMENT TO THE DIRECTOR OF THE DEPARTMENT OF INSURANCE ANNUALLY; TO ESTABLISH CERTAIN REQUIREMENTS FOR A LICENSEE IN THE EVENT OF A CYBERSECURITY EVENT; TO REQUIRE A LICENSEE TO NOTIFY THE DIRECTOR OF CERTAIN INFORMATION IN THE EVENT OF A CYBERSECURITY EVENT; TO GRANT THE DIRECTOR THE POWER AND AUTHORITY TO EXAMINE AND INVESTIGATE A LICENSEE; TO PROVIDE THAT DOCUMENTS, MATERIALS, OR OTHER INFORMATION IN THE CONTROL OR POSSESSION OF THE DEPARTMENT MUST BE TREATED AS CONFIDENTIAL AND TO AUTHORIZE THE DIRECTOR TO SHARE OR RECEIVE CONFIDENTIAL DOCUMENTS UNDER CERTAIN CIRCUMSTANCES; TO PROVIDE EXEMPTIONS FROM THE PROVISIONS OF THIS CHAPTER; TO PROVIDE PENALTIES

FOR VIOLATIONS; AND TO AUTHORIZE THE DIRECTOR TO PROMULGATE REGULATIONS.

Be it enacted by the General Assembly of the State of South Carolina:

SECTION 1. This act is known and may be cited as the "South Carolina Insurance Data Security Act".

SECTION 2. Title 38 of the 1976 Code is amended by adding:

"CHAPTER 99

South Carolina Insurance Data Security Act

Section 38-99-10. As used in this chapter:

(1) '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.

(2) 'Director' means the Director of the Department of Insurance or his designee.

(3) '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.

(4) 'Cybersecurity event' means an event resulting in unauthorized access to or the disruption or misuse of an information system or information stored on an information system. It 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. It 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.

(5) 'Department' means the Department of Insurance.

(6) '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.

(7) '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.

(8) ‘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 or process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

(9) ‘Licensee’ means an insurer, insurance broker, or an insurance producer 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.

(10) ‘Multi-factor authentication’ means authentication through verification of at least two of the following authentication factors:

(a) knowledge factors, such as a password; or

(b) possession factors, such as a token or text message on a mobile phone; or

(c) inherence factors, such as a biometric characteristic.

(11) ‘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) information concerning a consumer which because of name, number, personal mark, or other identifier can be used to identify the consumer, in combination with the consumer’s:

(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;

(c) 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.

(12) 'Person' means any individual or any nongovernmental entity including, but not limited, to a nongovernmental partnership, corporation, branch, agency, or association.

(13) 'Publicly available information' means 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 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 consumer has not done so.

(14) 'Risk assessment' means the risk assessment that each licensee is required to conduct under this chapter.

(15) 'State' means the State of South Carolina.

(16) '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.

Section 38-99-20. (A) A licensee must develop, implement, and maintain a comprehensive written information security program based on the licensee's risk assessment that contains administrative, technical, and physical safeguards for the protection of nonpublic information and the licensee's information system. The program must be 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.

(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.

(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 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) 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; and

(5) 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.

(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.

(2) include cybersecurity risks in the licensee's enterprise risk management process;

(3) 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;

(4) provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the licensee in the risk assessment; and

(5) 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;

(c) restricting access at physical locations containing nonpublic information to authorized individuals;

(d) protecting 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 by encryption or other appropriate means;

(e) adopting secure development practices for in-house developed applications used by the licensee and procedures for evaluating, assessing, 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) using effective controls, which may include multi-factor 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, 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.

(E)(1) If the licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum, require the

licensee's executive management or its delegates to develop, implement, and maintain the licensee's information security program and report in writing at least annually:

(a) the overall status of the information security program and the licensee's compliance with this chapter; 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, 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 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.

(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 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.

(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.

(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 clearly defined 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.

(I) A licensee domiciled in this State annually shall submit a written statement to the director no later than February fifteenth certifying that the insurer is in compliance with the requirements of this chapter. The licensee shall maintain and make available for examination by the department all records, schedules and data supporting this certificate for a period of five years. To the extent a licensee has identified areas, systems, or processes that require material improvement, updating, or redesign, the licensee shall document these identifications and the remedial efforts planned and underway to address these areas, systems, or processes.

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 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:

(1) complete an investigation pursuant to the requirements of this section; or

(2) 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.

Section 38-99-40 (A) A licensee shall notify the director 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 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 government 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 in electronic form as directed by the director and has a continuing obligation to update and supplement initial and subsequent notifications concerning the cybersecurity event:

(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 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) 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 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.

(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.

(D)(1) In the case of a cybersecurity event in a system maintained by a third-party service provider of which the licensee has become aware, the licensee shall treat such event as if the system was maintained by the licensee.

(2) The computation of 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 prevents or abrogates an agreement to fulfill any of the investigation requirements or notice requirements pursuant to the provisions of this chapter between a licensee and:

(a) another licensee;

(b) a third-party service provider; or

(c) any other party.

(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 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.

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 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 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 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 confidential 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.

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 independent contractors;

(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 a licensee considered to be in compliance with the provisions of this chapter under item (1) ceases to qualify for this consideration of being in compliance, he shall comply with the provisions of this chapter within one hundred eighty days.

Section 38-99-80. A licensee who violates a provision of this chapter is subject to penalties as provided in Section 38-2-10.

Section 38-99-90. The director is authorized to promulgate regulations necessary for the administration of this chapter."

SECTION 3. 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.

SECTION 4. 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 5. This act takes effect January 1, 2019, and upon approval by the Governor.

----XX----