South Carolina First State to Adopt NAIC Insurance Data Security Model Law

CYBERSECURITY AND PRIVACY | FINANCIAL SERVICES REGULATORY | LIFE, ANNUITY, AND RETIREMENT SOLUTIONS | SECURITIES & INVESTMENT COMPANIES | JUNE 24, 2018

On May 3, Governor Henry McMaster signed the *South Carolina Insurance Data Security Act* , making South Carolina the first state to adopt the NAIC Insurance Data Security Model Law.

South Carolina's law, which takes effect January 1, 2019, is substantially similar to the NAIC Model, which incorporated many of the requirements of the New York Department of Financial Services Cybersecurity Requirements for Financial Services Companies Regulation. Licensees will have until July 1, 2019 to, among other things, implement an information security program and establish an incident response plan. By July 1, 2020, licensees will be expected to have a third-party service provider management system in place.

Rhode Island has also been considering the NAIC Model and other state regulators have expressed an interest in doing the same. Given that legislative sessions for this year will soon conclude, this will likely be an issue for next year's legislative calendars. While industry participants agree on the fundamental purposes of the legislation, they continue to insist that to be workable, future efforts must focus on insuring uniformity and consistency across the various jurisdictions. If that is not achieved, the insurance industry will face the cost and burden of yet another set of patchwork requirements.

Similar to the NAIC Model, the South Carolina Act ("the Act"), also sets forth "standards for data security and standards for the investigation of and notification to the Commissioner of a Cybersecurity Event applicable to Licensees…." The Act applies to all licensees, defined as individuals or non-governmental entities required to be authorized, registered, or licensed pursuant to the state's insurance laws. There are very limited exceptions to the definition. The Act also requires that all licensees develop, implement, and maintain a comprehensive written information security program (ISP).

The ISP should be based on an entity's individual risk assessment and be commensurate with the licensee's size and complexity, the nature and scope of its activities, and the sensitivity of the nonpublic information used or in the licensee's possession, custody, or control. Nonpublic Information includes information that is not publicly available and covers material business information of the licensee as well as specified personal, financial, and health information concerning a consumer or family member.

The Act requires oversight by the board of directors or an appropriate board committee, the designation of a responsible person for the ISP, and due diligence and oversight of all third-party service providers. A licensee must also monitor its program to adjust for changes in threats and technology and must establish a written incident response plan.

The Act includes specific requirements for investigation and notification to the Director of the Department of Insurance, or his designee, in the case of a cybersecurity event. A cybersecurity event is defined as an event resulting in unauthorized access to, disruption, or misuse of an information system or information stored on such system. It does not include encrypted information where the key has not been acquired, released, or used, or events where the licensee has determined that the nonpublic information has not been used or released and has been returned or destroyed. Notification to the Director by all South Carolina domiciled licensees and licensees having 250 or more insureds in South Carolina is required within 72 hours from determining a cybersecurity event has occurred. Notification to affected consumers is governed by the state's general data breach and other applicable notification laws with copies of such notices provided to the Director.

A licensee is required to certify to the Director annually (no later than February 15) that it is in compliance with the information security program requirements of the South Carolina Insurance Data Security Act § 38-99-20, as well as maintain the materials and documentation used to support the certification for five years.

The Act **exempts** from the law a licensee with fewer than 10 employees (including any independent contractors), an

employee, agent, representative or designee of a licensee, who is also a licensee but is covered by the information security program of the other license, and HIPAA covered entities that certify compliance with the Act. This contrasts with the NAIC Model, which does not provide for an exemption, but includes three **exceptions** from the information security program requirements for (i) a licensee with fewer than 10 employees (including independent contractors), (ii) licensees who certify in writing that they have established and maintain an ISP that meets HIPAA requirements, and (iii) a licensee who is an employee, agent, representative, or designee of another licensee, but is covered by that licensee's ISP as long as that program complies with the information security program requirements. This deviation from the NAIC Model may require further guidance from the South Carolina Department of Insurance.

The NAIC Model is in play in other states as well. On June 6, Rhode Island's Senate Commerce Committee recommended that S. 2497, An Act Relating to Insurance – Insurance Data Security Act (introduced March 1, 2018) be postponed indefinitely. Instead, the Committee recommends further study of a substitute bill, S. 2497A (filed on June 6, 2018).

The South Carolina Insurance Data Security Act (H.B. 4655) is available here.

The NAIC Insurance Data Security Model Law is available here.