Independent Insurance Agents & Brokers of South Carolina

July 2020

Independent Insurance Agents Guide Regarding Third-Party Service Providers

The South Carolina Insurance Data Security Act (SCIDSA) requires that non-exempt licensees must exercise due diligence in selecting third-party service providers (TPSP) and establish additional oversight of third-party service providers on or before July 1, 2020. This oversight is to ensure selected TPSP implement appropriate administrative, technical and physical measures to protect and secure the information system and nonpublic information (NPI) that are accessible to, or held by, the TPSP. Third-party service providers have been responsible for most of the cyber event notifications the South Carolina Department of Insurance has received to date.

IIABSC has put together the information below to help our members comply, as well as a short TPSP questionnaire that can be sent to the agency's TPSP's to provide information on their cyber-security measures.

What information is covered?

Non-Public Personal Information:

"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 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;

(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.

Who is a third party?

S.C. Code Ann. Section 38-99-10 (2018).

A **third-party service provider** is defined as *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*.

This may include business arrangements between a licensee and another person (by contract or otherwise) that involve outsourced products and services, use of independent consultants, networking arrangements, merchant paying processing services, services provided by affiliates and subsidiaries, joint ventures, and other arrangements where the TPSP has an ongoing relationship with the licensee and access to the licensee's NPI.

Third-party relationships do not include customer or policyholder relationships. (Third parties for an insurance agency would NOT be a carrier or an MGA – they are licensees)

The SCIDSA requires licensees to implement and exercise effective risk management in their third-party relationships. A licensee's use of TPSPs does not diminish the licensee's responsibility through its Board of Directors or senior management to ensure that the TPSP is effectively safeguarding NPI in accordance with the SCIDSA and other applicable law.

What is the requirement regarding Third Parties:

Agencies must use "due diligence" in selecting the TPSP's they do business with. (Due diligence is not defined in our statute)

Agencies are expected to actively and continually engage in a process to identify, measure, monitor, and control the risks associated with third-party relationships. This process is expected to be proportionate to the agency's size and complexity, as well as the nature and scope of the agency's activities therefore the "process" may be somewhat different for each agency.

Agencies must require TPSP to implement appropriate administrative, technical and physical measures to protect and secure the information system and nonpublic information that are accessible to, or held by, the third-party service provider.

The SC DOI has jurisdiction over all situations in which an agency arranges, by contract or otherwise, for the performance of any applicable functions of its operations. The Department may use its authority to examine the functions or operations performed by a third-party on the agency's behalf to the same extent as if they were performed by the agency itself on its own premises.

Recommendations for dealing with Third-parties*

Request a copy of the third-party's data security protection program and review it to assure compliance with the SCIDSA. Some considerations could be:

- Does the third-party have sufficient experience in identifying, assessing, and mitigating known and emerging threats and vulnerabilities in its own systems.
- Review the third-party's certifications of compliance with applicable cyber security practices such as NIST, ISO, GDPR, etc.
- Request a certification that a vulnerability security audit has been completed in the past 12 months by a qualified party that shows that no vulnerabilities are present or they have been addressed. Secure documentation of those results.
- Consider using a TPSP Questionnaire (IIABSC has developed one) that addresses the adequacy of the TPSP's cybersecurity program.

Assess the third-party's ability to respond to service disruptions resulting from natural disasters, human error, or intentional physical or cyber-attacks.

Review the third-party's incident reporting and management program.

Review the agency's contract with TPSP's and/or provide the TPSP with terms and conditions to include the following:

  - *A requirement the TPSP comply with all applicable laws, regulations, and industry standards;*
  - *Define and require the TPSP to meet a minimum standard of care based on applicable laws or regulations as well as the licensee's policies and procedures;*

- *Permit the TPSP to access the licensee's IT systems and use its data only to perform work set forth in the agreement;*
- *Prohibit the TPSP from disclosing or sharing data with any other third-parties without your consent. Include how to address data requests from regulators and other governmental authorities;*
- *Require the TPSP to pass the privacy and data security obligations on to any subcontractors the TPSP uses to perform the work required by the contract;*
- *Require the TPSP to return or destroy, at the licensee's request, all copies of the licensee's data on termination of the agreement;*
- *Define specific security incident reporting and response requirements, including cost allocation and responsibilities for handing data breaches and liabilities;*
- *Require TPSP to give licensee the right to audit or otherwise review or assess the TPSP's privacy and data security practices; and*
- *Include provisions that address risk allocations including:*
    - *Indemnification and hold harmless clauses;*
    - *Cyber insurance requirements, including specific limits; and*
    - *Allocation of costs for regulatory penalties and consumer notifications.*

Third-party should be advised that the performance of services for the agency by the third-party are subject to SC DOI examination and oversight.

Additional recommendations the agency may want to consider:

Check compliance status with regulators and self-regulatory organizations as appropriate.

Assess the third-party's financial condition, including reviews of the third-party's audited financial statements.

**These recommendations are for informational purposes only and are not intended to constitute legal advice. The purpose is to outline issues that the agency should consider when reviewing the use of third-party service providers. Agencies should contact their attorney for legal advice on issues relating to their informational security program.*