Title 23. Public Utilities and Regulated Industries

Chapter I. State Insurance Department, Department of Commerce

Subchapter A. Generally

Part 31. Standards for Safeguarding Customer Information

Codification Notes. This part as promulgated prior to codification into the Code of Arkansas Rules provided as follows:

"Section 2. Authority

This rule is promulgated pursuant to the authority granted by Sections 23-61-108, 23-61-113, 23-66-207, 25-15-203—204 of the Arkansas Code Annotated, and other applicable laws or rules."

"Section 12. Effective Date

This rule shall be effective on September 20, 2002."

Subpart 1. Generally

23 CAR § 31-101. Preamble.

(a) This part establishes standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information, pursuant to Sections 501, 505(b), and 507 of the Gramm-Leach-Bliley Act, codified at 15 U.S.C. §§ 6801, 6805(b), and 6807.

(b)(1) Section 501(a) provides that it is the policy of the United States Congress that each financial institution has an affirmative and continuing obligation to:

(A) Respect the privacy of its customers; and

(B) Protect the security and confidentiality of those customers' nonpublic personal information.

(2) Section 501(b) requires the state insurance regulatory authorities to establish appropriate standards relating to administrative, technical and physical safeguards to:

(A) Ensure the security and confidentiality of customer records and information;

(B) Protect against any anticipated threats or hazards to the security or integrity of such records; and

(C) Protect against unauthorized access to or use of records or information that could result in substantial harm or inconvenience to a customer.

(c) Section 505(b)(2) calls on state insurance regulatory authorities to implement the standards prescribed under Section 501(b) by rules with respect to persons engaged in providing insurance.

(d)(1) Section 507 provides, among other things, that a state rule may afford persons greater privacy protections than those provided by Subtitle A of Title V of the Gramm-Leach-Bliley Act.

(2) This part requires that the safeguards established pursuant to this part shall apply to nonpublic personal information, including nonpublic personal financial information and nonpublic personal health information, about customers and nonpublic personal information contained on applications for an insurance product submitted to a licensee by a consumer, regardless of whether the insurance product is ultimately purchased by the consumer.

Authority. Arkansas Code § 23-61-108.

Codification Notes. Gramm-Leach-Bliley Act was enacted by Pub. L. No. 106-102.

23 CAR § 31-102. Definitions.

For purposes of this part, the following definitions apply:

(1) "Customer" means a customer as defined in 23 CAR § 30-103(9);

(2)(A) "Customer information" means nonpublic personal information, as defined in 23 CAR § 30-103(21), about a customer, whether in paper, electronic, or other form, that is maintained by or on behalf of the licensee.

(B) For purposes of this part, customer information shall also include nonpublic personal information contained in applications for an insurance product submitted to a licensee by a consumer, as defined in 23 CAR § 30-103(6), regardless of whether the insurance product is ultimately purchased by the consumer;

(3) "Customer information systems" means the electronic or physical methods used to access, collect, store, use, transmit, protect, or dispose of customer information;

(4) "Licensee" means a licensee as that term is defined in 23 CAR § 30-103(17), except that "licensee" shall not include:

(A) A purchasing group; or

(B) An unauthorized insurer in regard to the excess line business conducted pursuant to Arkansas Code § 23-65-301 et seq.; and

(5) "Service provider" means a person that maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to the licensee.

Authority. Arkansas Code § 23-61-108.

23 CAR § 31-103. Information security program.

(a) Each licensee shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards for the protection of customer information.

(b) The administrative, technical, and physical safeguards included in the information security program shall be appropriate to the size and complexity of the licensee and the nature and scope of its activities.

Authority. Arkansas Code § 23-61-108.

23 CAR § 31-104. Objectives of information security program.

A licensee's information security program shall be designed to:

(1) Ensure the security and confidentiality of customer information;

(2) Protect against any anticipated threats or hazards to the security or integrity of the information; and

(3) Protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer.

Authority. Arkansas Code § 23-61-108.

23 CAR § 31-105. Examples of methods of development and implementation.

(a) The actions and procedures described in 23 CAR §§ 31-106 – 31-109 are examples of methods of implementation of the requirements of 23 CAR §§ 31-103 and 31-104.

(b) These examples are nonexclusive illustrations of actions and procedures that licensees may follow to implement 23 CAR §§ 31-103 and 31-104.

Authority. Arkansas Code § 23-61-108.

23 CAR § 31-106. Assess risk.

The licensee:

(1) Identifies reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems;

(2) Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and

(3) Assesses the sufficiency of policies, procedures, customer information systems, and other safeguards in place to control risks.

Authority. Arkansas Code § 23-61-108.

23 CAR § 31-107. Manage and control risk.

The licensee:

(1) Designs its information security program to control the identified risks, commensurate with the sensitivity of the information, as well as the complexity and scope of the licensee's activities;

(2) Trains staff, as appropriate, to implement the licensee's information security program; and

(3)(A) Regularly tests or otherwise regularly monitors the key controls, systems, and procedures of the information security program.

(B) The frequency and nature of these tests or other monitoring practices are determined by the licensee's risk assessment.

Authority. Arkansas Code § 23-61-108.

23 CAR § 31-108. Oversee service provider arrangements.

The licensee:

(1) Exercises appropriate due diligence in selecting its service providers; and

(2) Requires its service providers to implement appropriate measures designed to meet the objectives of this part.

Authority. Arkansas Code § 23-61-108.

23 CAR § 31-109. Adjust the program.

The licensee monitors, evaluates, and adjusts, as appropriate, the information security program in light of any relevant changes in:

(1) Technology;

(2) The sensitivity of its customer information;

(3) Internal or external threats to information; and

(4) The licensee's own changing business arrangements, such as:

(A) Mergers and acquisitions;

(B) Alliances and joint ventures;

(C) Outsourcing arrangements; and

(D) Changes to customer information systems.

Authority. Arkansas Code § 23-61-108.

23 CAR § 31-110. Determined violation.

A violation of this part shall be deemed to be an unfair method of competition or an unfair or deceptive act and practice in this state, in violation of Arkansas Code § 23-66-201 et seq.

Authority. Arkansas Code §§ 23-61-108, 23-67-207.

23 CAR § 31-111. Compliance date.

Each licensee shall establish and implement an information security program, including appropriate policies and systems, pursuant to this part by January 1, 2003.

Authority. Arkansas Code § 23-61-108.