230-RICR-20-60-8

TITLE 230 – DEPARTMENT OF BUSINESS REGULATION

CHAPTER 20 – INSURANCE

SUBCHAPTER 60 – MISCELLANEOUS

Part 8 - Standards for Safeguarding Customer Information

8.1. Authority

This Regulation is promulgated pursuant to R.I. Gen. Laws §§ 27-58-4, 11-49.2-1 et seq. and 42-35-3. This Regulation applies only to licensees subject to the jurisdiction of the Department of Business Regulation and not those subject to the jurisdiction of the Officer of the Hearing Insurance Commissioner as indicated in R.I. Gen. Laws §§ 42-14-5(d) and 42-14.5-1 et seq.

8.2. Purpose and Scope

A. This Regulation 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 ("GLBA") at 15 U.S.C. §§ 6801, 6805(b) and 6807.

B. Section 501(a) of GLBA provides that it is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information. Section 501(b) requires the state insurance regulatory authorities establish appropriate standards relating to administrative, technical and physical safeguards:

1. to ensure the security and confidentiality of customer records and information;

2. to protect against any anticipated threats or hazards to the security or integrity of such records; and

3. to 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) of GLBA calls on state insurance regulatory authorities to implement the standards prescribed under Section 501(b) by regulation with respect to persons engaged in providing insurance.

D. Section 507 of GLBA provides, among other things, that a state regulation may afford persons greater privacy protections than those provided by subtitle A of Title V of GLBA. This Regulation requires that the safeguards established pursuant to this Regulation shall apply to nonpublic personal information, including nonpublic personal financial information and nonpublic personal health information.

8.3. Definitions

A. For purposes of this Part, the following definitions apply:

1. "Customer" means a customer of the licensee as the term customer is defined in § 7.4(H) of this Subchapter.

2. "Customer information" means nonpublic personal financial information as defined in § 7.4(A)(20) of this Subchapter and nonpublic personal health information as defined in § 7.4(A)(21) of this Subchapter about a customer, whether in paper, electronic or other form, that is maintained by or on behalf of the licensee.

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 § 7.4(A)(17) of this Subchapter except that "licensee" shall not include: a purchasing group; or an unauthorized insurer in regard to the surplus line business conducted pursuant to R.I. Gen. Laws § 27-3-38 through 27-3-42.

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.

8.4. Information Security Program

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

8.5. Objectives of Information Security Program

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

1. Insure 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.

8.6. Examples of Methods of Development and Implementation

The actions and procedures described in §§ 8.7 through 8.10 of this Part are examples of methods of implementation of the requirements of §§ 8.4 and 8.5 of this Part. These examples are non-exclusive illustrations of actions and procedures that licensees may follow to implement §§ 8.4 and 8.6 of this Part.

8.7. Assess Risk

A. 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.

8.8. Manage and Control Risk

A. 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. Regularly tests or otherwise regularly monitors the key controls, systems and procedures of the information security program. The frequency and nature of these tests or other monitoring practices are determined by the licensee's risk assessment.

8.9. Oversee Service Provider Arrangements

A. 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 regulation, and, where indicated by the licensee's risk assessment, takes appropriate steps to confirm that its service providers have satisfied these obligations.

8.10. Adjust the Program

The licensee monitors, evaluates and adjusts, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to customer information systems.

8.11 Notification of Breach of Security System

A licensee that is required to send a disclosure of a breach of the security of computerized unencrypted data that poses a significant risk of identity theft pursuant to Rhode Island Identity Theft Protection Act of 2005 (R.I. Gen Laws § 11-49.2-3) is also required to send a notice of the breach to the Rhode Island Department of Business. The disclosure to the Department shall be made in the most expedient time possible and without unreasonable delay consistent with the disclosure required in the R.I. Gen. Laws §11-49.2-3.

8.12. Severability

If any section, term, or provision of this Part should be adjudged invalid for any reason, that judgment should not effect, impair, or invalidate any remaining section, term, or provision, which shall remain in full force and effect.

230-RICR-20-60-8

TITLE 230 - DEPARTMENT OF BUSINESS REGULATION (INCLUDES THE OFFICE OF THE HEALTH INSURANCE COMMISSIONER)

CHAPTER 20 - INSURANCE

SUBCHAPTER 60 - MISCELLANEOUS

PART 8 - Standards for Safeguarding Customer Information (230-RICR-20-60-8)

Type of Filing: Technical Revision
Effective Date: 09/01/2006

Editorial Note: This Part was filed with the Department of State prior to the launch of the Rhode Island Code of Regulations. As a result, this digital copy is presented solely as a reference tool. To obtain a certified copy of this Part, contact the Administrative Records Office at (401) 222-2473.