R590. Insurance, Administration.
R590-216. Standards for Safeguarding Customer Information.
R590-216-1. Authority.

This rule is promulgated pursuant to Subsections 31A-2-202(1), 31A-2-201(2) and 31A-2-201(3)(a) in which the commissioner is empowered to administer and enforce Title 31A, to perform duties imposed by Title 31A and to make administrative rules to implement the provisions of Title 31A. Furthermore, Title V, Section 505 (15 United States Code (U.S.C.) 6805)) empowers the Utah Insurance Commissioner to enforce Subtitle A of Title V of the Gramm-Leach-Bliley Act of 1999(15 U.S.C. 6801 through 6820). Title V, Section 505 (15 U.S.C. 6805(b)(2)) authorizes the commissioner to issue rules to implement the requirements of Title V, Section 501(b)of the federal act. The commissioner is also authorized under Subsection 31A-23a-417(3) to adopt rules implementing the requirements of Title V, Section 501(b) of the federal act.

R590-216-2. Purpose and Scope.

(1) This rule establishes standards applicable to the department's licensees to assist them in 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.

(2) Section 501(a) 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 to establish appropriate standards relating to administrative, technical and physical safeguards:

(a) to ensure the security and confidentiality of customer records and information;

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

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

(3) Under Section 505(b)(2) state insurance regulatory authorities are to implement the standards prescribed under Section 501(b) by rule with respect to persons engaged in providing insurance.

(4) 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. This rule requires that the safeguards established pursuant to the rule shall apply to nonpublic personal information, including nonpublic personal financial information and nonpublic personal health information that licensees of the department obtain from their customers.

R590-216-3. Definitions.

For purposes of this rule, the following definitions apply:

(1) "Customer" means a customer of the licensee as the term customer is defined in Rule R590-206, Privacy of Consumer Financial and Health Information Rule, Subsection 4(9).

(2) "Customer information" means nonpublic personal information as defined in Subsection R59-206-4(19) 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 Subsection R590-206-4(17)(a), except that "licensee" shall not include: a purchasing group; manufacturer or seller warranty provider and manufacturer or seller service contract provider exempted by R590-210, Privacy of Consumer Information Exemption for Manufacturer Warranties and Service Contract; or an unauthorized insurer in regard to the excess line business conducted pursuant to Section 31A-15-103.

(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.

R590-216-4. 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.

R590-216-5. 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.

R590-216-6. Examples of Methods of Development and Implementation.

The actions and procedures described in this section are examples of methods of implementation of the requirements of Sections 4 and 5 of this rule. These examples are non-exclusive illustrations of actions and procedures that licensees may adopt to implement Sections 4 and 5 of this rule.

(1) For risk assessment, the licensee may:

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

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

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

(2) For risk management and control, the licensee may:

(a) design 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;

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

(c) regularly test or otherwise regularly monitor 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.

(3) For service provider arrangement oversight, the licensee may:

(a) exercise appropriate due diligence in selecting its service providers; and

(b) require its service providers to implement appropriate measures designed to meet the objectives of this rule, and, where indicated by the licensee's risk assessment, takes appropriate steps to confirm that its service providers have satisfied these obligations.

(4) For program adjustment, the licensee may monitor, evaluate and adjust, 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.

R590-216-7. Determined Violation.

Violation of any provision of the rule will result in appropriate enforcement action by the department, which may include forfeiture, penalties, and revocation of license as provided in Section 31A-2-308.

R590-216-8. Enforcement Date.

The commissioner will begin enforcing the provisions of this rule 120 days from the effective date of the rule.

KEY: insurance
Date of Enactment or Last Substantive Amendment: September 26, 2002
Notice of Continuation: August 18, 2017
Authorizing, and Implemented or Interpreted Law: 31A-2-201; 31A-2-202; 31A-23a-417; 15 U.S.C. 6801; 15 U.S.C. 6805; 15 U.S.C. 6807