State of Utah
Administrative Rule Analysis
Revised June 2022

NOTICE OF PROPOSED RULE		
TYPE OF RULE: New ___; Amendment _x_; Repeal ___; Repeal and Reenact ___		
Title No. - Rule No. - Section No.		
Rule or Section Number:	**R590-216**	**Filing ID: Office Use Only**

Agency Information

1. Department:	Insurance	
Agency:	Administration	
Room number:	Suite 2300	
Building:	Taylorsville State Office Building	
Street address:	4315 S. 2700 W.	
City, state and zip:	Taylorsville, UT 84129	
Mailing address:	PO Box 146901	
City, state and zip:	Salt Lake City, UT 84114-6901	
Contact persons:		
Name:	**Phone:**	**Email:**
Steve Gooch	801-957-9322	sgooch@utah.gov
Please address questions regarding information on this notice to the agency.		

General Information

2. Rule or section catchline:

R590-216. Standards for Safeguarding Customer Information

3. Purpose of the new rule or reason for the change (Why is the agency submitting this filing?)**:**

The rule is being changed in compliance with Executive Order 2021-12. During the review of this rule, the department discovered a number of minor issues that needed to be amended.

4. Summary of the new rule or change (What does this filing do? If this is a repeal and reenact, explain the substantive differences between the repealed rule and the reenacted rule)**:**

The majority of the changes are being done to fix style issues to bring the rule text more in line with current rulewriting standards. Other changes make the language of the rule more clear, remove the Determined Violation and Enforcement sections, and add a Severability section. The changes do not add, remove, or change any regulations or requirements.

Fiscal Information

5. Provide an estimate and written explanation of the aggregate anticipated cost or savings to:

A) State budget:

There is no anticipated cost or savings to the state budget. The changes are largely clerical in nature, and will not change how the department functions.

B) Local governments:

There is no anticipated cost or savings to local governments. The changes are largely clerical in nature, and will not affect local governments.

C) Small businesses ("small business" means a business employing 1-49 persons)**:**

There is no anticipated cost or savings to small businesses. The changes are largely clerical in nature, and will not affect small businesses.

D) Non-small businesses ("non-small business" means a business employing 50 or more persons)**:**

There is no anticipated cost or savings to non-small businesses. The changes are largely clerical in nature, and will not affect non-small businesses.

E) Persons other than small businesses, non-small businesses, state, or local government entities ("person" means any individual, partnership, corporation, association, governmental entity, or public or private organization of any character other than an ***agency***)**:**

There is no anticipated cost or savings to any other persons. The changes are largely clerical in nature.

F) Compliance costs for affected persons (How much will it cost an impacted entity to adhere to this rule or its changes?)**:**

There are no compliance costs for any affected persons. The changes are largely clerical in nature.

G) Regulatory Impact Summary Table (This table only includes fiscal impacts that could be measured. If there are inestimable fiscal impacts, they will not be included in this table. Inestimable impacts will be included in narratives above.)

Regulatory Impact Table

Fiscal Cost	**FY2023**	**FY2024**	**FY2025**
State Government	$0	$0	$0
Local Governments	$0	$0	$0
Small Businesses	$0	$0	$0
Non-Small Businesses	$0	$0	$0
Other Persons	$0	$0	$0
Total Fiscal Cost	**$0**	**$0**	**$0**
Fiscal Benefits	**FY2023**	**FY2024**	**FY2025**
State Government	$0	$0	$0
Local Governments	$0	$0	$0
Small Businesses	$0	$0	$0
Non-Small Businesses	$0	$0	$0
Other Persons	$0	$0	$0
Total Fiscal Benefits	**$0**	**$0**	**$0**
Net Fiscal Benefits	**$0**	**$0**	**$0**

H) Department head comments on fiscal impact and approval of regulatory impact analysis:

The Commissioner of Insurance, Jonathan T. Pike, has reviewed and approved this regulatory impact analysis.

Citation Information

6. Provide citations to the statutory authority for the rule. If there is also a federal requirement for the rule, provide a citation to that requirement:

Section 31A-2-201	Section 31A-23a-417	

Incorporations by Reference Information

7. Incorporations by Reference (if this rule incorporates more than two items by reference, please include additional tables)**:**

A) This rule adds, updates, or removes the following title of materials incorporated by references (a copy of materials incorporated by reference must be submitted to the Office of Administrative Rules; *if none, leave blank*)**:**

Official Title of Materials Incorporated (from title page)	
Publisher	
Issue Date	
Issue or Version	

B) This rule adds, updates, or removes the following title of materials incorporated by references (a copy of materials incorporated by reference must be submitted to the Office of Administrative Rules; *if none, leave blank*)**:**

Official Title of Materials Incorporated (from title page)	
Publisher	
Issue Date	

Issue or Version	

Public Notice Information

8. The public may submit written or oral comments to the agency identified in box 1. (The public may also request a hearing by submitting a written request to the agency. See Section 63G-3-302 and Rule R15-1 for more information.)		
A) Comments will be accepted until:		**05/31/2023**
B) A public hearing (optional) will be held:		
On (mm/dd/yyyy)**:**	**At** (hh:mm AM/PM)**:**	**At** (place)**:**

9. This rule change MAY become effective on:	**06/07/2023**
NOTE: The date above is the date the agency anticipates making the rule or its changes effective. It is NOT the effective date.	

Agency Authorization Information

To the agency: Information requested on this form is required by Sections 63G-3-301, 302, 303, and 402. Incomplete forms will be returned to the agency for completion, possibly delaying publication in the *Utah State Bulletin* and delaying the first possible effective date.			
Agency head or designee and title:	Steve Gooch, Public Information Officer	**Date:**	**04/14/2023**

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.~~]This rule is promulgated by the commissioner pursuant to Sections 31A-2-201 and 31A-23a-417.

R590-216-2. Purpose and Scope.

(1) [~~This rule establishes standards applicable to the department's licensees to assist them~~]The purpose of this rule is to establish standards to assist a licensee 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~~] under 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.~~]

(2) This rule applies to a licensee of the department that obtains any nonpublic information from a customer, including:

(a) nonpublic personal financial information; or

(b) nonpublic personal health information.

R590-216-3. Definitions.

[~~For purposes of this rule, the following definitions apply:~~]Terms used in this rule are defined in Section 31A-1-301. Additional terms are defined as follows:

(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)~~]Section R590-206-4.

(2) "Customer information" [~~means~~]has the same meaning as "nonpublic personal information" as defined in [~~Subsection R59-206-4(19)~~]Section R590-206-4 about a customer, whether in paper, electronic, or other form, that is maintained by or on behalf of the licensee.

(3) "Customer information system[~~s~~]" means [~~the~~]any electronic or physical method[~~s~~] used to access, collect, store, use, transmit, protect, or dispose of customer information.

(4)(a) "Licensee" means a licensee as [~~that term is~~]defined in [~~Subsection R590-206-4(17)(a), except that "licensee" shall not include:~~]Section R590-206-4.

(b) "Licensee" does not mean:

(i) a purchasing group;

(ii) a manufacturer or seller warranty provider [~~and~~]or manufacturer or seller service contract provider exempted by [~~R590-210, Privacy of Consumer Information Exemption for Manufacturer Warranties and Service Contract~~]Section R590-206-2; or

(iii) an unauthorized insurer [~~in regard to~~]regarding the excess line business conducted pursuant to Section 31A-15-103.

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

R590-216-4. Information Security Program.

[~~Each~~](1) A licensee shall implement a comprehensive written information security program [~~that includes~~]including administrative, technical, and physical safeguards [~~for the protection of~~]to protect customer information.

(2) 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~~]ensure the security and confidentiality of customer information;

(2) [~~Protect~~]protect against any anticipated [~~threats or hazards~~]threat or hazard to the security or integrity of the information; and

(3) [~~Protect~~]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 purposes of risk assessment, [~~the~~]a 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 purposes of risk management and control, [~~the~~]a licensee may:

(a) design its information security program to control the identified risks, [~~commensurate~~]consistent 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~~], the frequency and nature of which shall be determined by the licensee's risk assessment.

(3) For purposes of service provider arrangement oversight, [~~the~~]a 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~~]take appropriate steps to confirm that its service providers have satisfied these obligations.

(4) For purposes of program adjustment, [~~the~~]a licensee may monitor, evaluate, and adjust[~~, as appropriate,~~] the information security program [~~in light of any~~]considering:

(a) any relevant change[~~s~~] in technology[~~,~~];

(b) the sensitivity of its customer information[~~,~~];

(c) any internal or external threat[~~s~~] to information[~~,~~]; and

(d) the licensee's [~~own~~]changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems.

(5) Subsections (1) through (4) are examples of implementation methods. A licensee may adopt other actions or procedures to implement Sections R590-216-4 and R590-216-5.

[~~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.~~]

R590-216-7. Severability.

If any provision of this rule, Rule R590-216, or its application to any person or situation is held invalid, such invalidity does not affect any other provision or application of this rule that can be given effect without the invalid provision or application. The remainder of this rule shall be given effect without the invalid provision or application.

KEY: insurance
Date of Last Change: September 26, 2002
Notice of Continuation: August 17, 2022
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