

State of Rhode Island and Providence Plantations
DEPARTMENT OF BUSINESS REGULATION
Division of Insurance
233 Richmond Street
Providence, RI 02903

NOTICE OF PROPOSED REGULATION
AND NOTICE OF PUBLIC HEARING

Notice is hereby given, in accordance with R.I. Gen. Laws §§ 42-14-17 and 42-35-3, that the Department of Business Regulation (“DBR”) proposes to enact the following Regulation:

Insurance Regulation 105 – Standards for Safeguarding Consumer Information

The enactment is intended to require licensees to take steps to safeguard consumer information. The regulation is based upon National Association of Insurance Commissioners Model 673 which has been adopted by approximately thirty states. The highlighted portion of the proposed regulation is Rhode Island specific language designed to address notification to consumers when security is breached and is intended to be in conformance with R.I.G.L. § 11-49.2-1 *et seq.*

Notice is also hereby given, in accordance with R.I. Gen. Laws § 42-35-2, that DBR will hold a public hearing beginning at 9:00 a.m. on September 8, 2005 in the Main Hearing Room of the Department of Business Regulation, 233 Richmond Street, Providence, Rhode Island 02903, regarding the Proposed Regulations.

Copies of the Proposed Regulation is on file at the Department and copies may be obtained from the Legal Division, Department of Business Regulation, 233 Richmond Street, Providence, Rhode Island 02903 during normal working hours on regular business days or by mail upon request. The Proposed Regulation may also be obtained from DBR’s website www.dbr.state.ri.us.

In the development of the Proposed Regulations, consideration was given to overlapping approaches, overlap and duplication with other statutory and regulatory provisions and economic impact on small business and cities and towns.

All interested persons may submit their views, data or arguments regarding the Proposed Regulations, including information relating to alternative approaches, duplication or overlap with other state rules or regulations and the economic impact of the Regulations on small business and/or cities and towns, orally at the public hearing or in writing, either by delivering the same in person or United States mail with postage pre-paid thereon to the Department of Business Regulation, 233 Richmond Street, Providence, Rhode Island 02903 attention Elizabeth Kelleher Dwyer, Hearing Officer or by e-mail to elizabeth_dwyer@dbr.state.ri.us

ALL SUBMISSIONS MUST BE RECEIVED NOT LATER THAN SEPTEMBER 8, 2005
AT 9:00 A.M.

The hearing room is accessible to the handicapped. Individuals requesting interpreter services for the hearing impaired must notify the Office of Legal Counsel at (401) 222 5400 or TDD (401) 222 2999 not less than ninety-six (96) hours in advance of the hearing date.

A. Michael Marques
Director, Department of Business Regulation

INSURANCE REGULATION 105
STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

Table of Contents

Section 1.	Authority
Section 2.	Purpose and Scope
Section 3.	Definitions
Section 4.	Information Security Program
Section 5.	Objectives of Information Security Program
Section 6.	Examples of Methods of Development and Implementation
Section 7.	Assess Risk
Section 8.	Manage and Control Risk
Section 9.	Oversee Service Provider Arrangements
Section 10.	Adjust the Program
Section 11.	Severability
Section 12.	Effective Date

Section 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.

Section 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.

Section 3. Definitions

For purposes of this Regulation, the following definitions apply:

- A. “Customer” means a customer of the licensee as the term customer is defined in Insurance Regulation 99(4)(H).
- B. “Customer information” means nonpublic personal financial information as defined in Regulation 99(P) and nonpublic personal health information as defined in Regulation 100 3(K) about a customer, whether in paper, electronic or other form, that is maintained by or on behalf of the licensee.
- C. “Customer information systems” means the electronic or physical methods used to access, collect, store, use, transmit, protect or dispose of customer information.
- D. “Licensee” means a licensee as that term is defined in Regulation 99(N) and Regulation 100(I) 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.
- E. “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.

Section 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.

Section 5. Objectives of Information Security Program

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

- A. Ensure the security and confidentiality of customer information;

- B. Protect against any anticipated threats or hazards to the security or integrity of the information; and
- C. Protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer.

Section 6. Examples of Methods of Development and Implementation

The actions and procedures described in Sections 7 through 10 of this Regulation are examples of methods of implementation of the requirements of Sections 4 and 5 of this Regulation. These examples are non-exclusive illustrations of actions and procedures that licensees may follow to implement Sections 4 and 6 of this Regulation.

Section 7. Assess Risk

The licensee:

- A. Identifies reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems;
- B. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and
- C. Assesses the sufficiency of policies, procedures, customer information systems and other safeguards in place to control risks.

Section 8. Manage and Control Risk

The licensee:

- A. 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;
- B. Trains staff, as appropriate, to implement the licensee's information security program; and
- C. 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.

Section 9. Oversee Service Provider Arrangements

The licensee:

- A. Exercises appropriate due diligence in selecting its service providers; and
- B. 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.

Section 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.

Section 11. Notification of Breach of Security System

- A. The licensee shall disclose any breach of the security of the system which poses a significant risk of identity theft following discovery or notification of the breach in the security of the data to any person whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person or a person without authority, to acquire such information. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the exceptions in subsection B below and with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
- B. The notification required by subsection A above may be delayed or not required in accordance with the legitimate needs of law enforcement as set forth in R.I.G.L. § 11-49.2-3 and R.I.G.L. § 11-49.2-4 respectively.
- C. The licensee shall notify and provide all relevant information to the Department as soon as possible following any breach in security as described in subsection A above. If the licensee notified or intends to notify persons affected by a breach, it shall supply a complete description of the notification as well as the manner and time of notification. If notification was not made the licensee will provide a complete justification of why notification was not made.

Section 12. Severability

If any section, term, or provision of this Regulation 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.

Section 13. Effective Date

Each licensee shall establish and implement an information security program, including appropriate policies and systems pursuant to this Regulation by January 1, 2006.

EFFECTIVE DATE: September , 2005