INSURANCE
DEPARTMENT OF BANKING AND INSURANCE
DIVISION OF INSURANCE

Standards for Safeguarding Customer Information

Proposed New Rules: N.J.A.C. 11:1-44

Authorized By: Holly C. Bakke, Commissioner, Department of Banking and Insurance

Authority: N.J..S.A. 17:1-8.1, 17:1-15e, and 15 U.S.C. §§6801, 6805(b), and 6807

Calendar Reference: See Summary below for explanation of exception to calendar requirement.

Proposal Number: PRN 2003-92

Submit comments by May 2, 2003 to:

Douglas A. Wheeler
Assistant Commissioner
Legislative and Regulatory Affairs
New Jersey Department of Banking and Insurance
20 West State Street
P.O. Box 325
Trenton, NJ 08625-0325
Fax: (609) 292-0896
E-mail: legsregs@dobi.state.nj.us

The agency proposal follows:

Summary

The Gramm-Leach-Bliley Act, P.L. 106-102 (GLBA), enacted November 12, 1999, requires, among other things, financial institutions, including insurers, to protect the privacy of consumers' non-public personal information. 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 information. Furthermore, Section 501(b) requires Federal and State

regulators to implement GLBA's privacy protections with respect to the entities that they regulate. Specifically, Section 501(b) requires each agency or authority to establish appropriate standards for the financial institutions subject to their jurisdiction 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 such records or information which could result in substantial harm or inconvenience to any customer.

Various Federal agencies have already established rules with respect to the entities under their respective jurisdictions as follows: the United States Department of the Treasury, Office of the Comptroller of the Currency; the Federal Reserve System; the Federal Deposit Insurance Corporation; the Department of the Treasury, Office of Thrift Supervision; the Federal Trade Commission; and National Credit Union Administration.

Under Section 507, state insurance regulators are authorized to enforce Federal privacy laws as they apply to insurers and may enact and enforce privacy standards that exceed those that exist in GLBA. Existing law in New Jersey regarding disclosure of information gathered by insurers meets or exceeds Federal standards. N.J.S.A. 17:23A-1 et seq., effective December 7, 1985, regulates the collection, use and disclosure of information gathered by insurers in connection with policies, contracts or certificates of insurance issued or delivered in this State.

The Department now proposes these new rules with respect to insurers, producers and other licensees under Title 17 or 17B of the New Jersey Statutes to provide standards for development and implementation of administrative, technical and physical safeguards to protect the security, confidentiality and integrity of customer information, as required by GLBA. These proposed new rules are based on a model rule adopted by the National Association of Insurance Commissioners

(NAIC), and thus reflect the consensus and national standard regarding the development of standards for safeguarding customer information by insurers and other applicable licensees. The proposed new rules do not affect the duty of a licensee to maintain information as confidential pursuant to law, including, but not limited to, N.J.S.A. 17:23A-1 et seq. Moreover, the proposed new rules define "nonpublic personal information" to mean "personal information" and "privileged information" as defined in N.J.S.A. 17:23A-2, which the Department believes is at least as broad as the definition in GLBA.

Proposed N.J.A.C. 11:1-44.1 sets forth the purpose and scope of the subchapter.

Proposed N.J.A.C. 11:1-44.2 sets forth the definitions of terms used throughout the subchapter.

Proposed N.J.A.C. 11:1-44.3 requires that each licensee implement a comprehensive written information security program that provides administrative, technical and physical safeguards for the protection of customer information appropriate to the size and complexity of the licensee and the nature and scope of its activities.

Proposed N.J.A.C. 11:1-44.4 sets forth the objectives of the information security program required to be implemented by licensees, which shall be designed to ensure the security and confidentiality of customer information; protect against any anticipated threats or hazards to the security or integrity of the information; and protect against unauthorized access or use of information that could result in substantial harm or inconvenience to any customer.

Proposed N.J.A.C. 11:1-44.5 requires that licensees assess the risk of threats to the confidentiality of information.

Proposed N.J.A.C. 11:1-44.6 requires that a licensee manage and control risk of disclosure of nonpublic information by: designing its information security program to control identified risks,

commensurate with the sensitivity of the information and the complexity and scope of licensee's activities; training staff to implement its information security program; and test or otherwise monitor key controls, systems and procedures of the security program.

Proposed N.J.A.C. 11:1-44.7 provides that a licensee must oversee its service provider agreements by exercising appropriate due diligence in selecting its service providers and requiring its service providers to implement appropriate measures designed to meet the objectives of this subchapter.

Proposed N.J.A.C. 11:1-44.8 requires that a licensee monitor, evaluate and adjust, as appropriate, its information security program in light of changes in technology, the sensitivity of its customer information, and other factors.

Proposed N.J.A.C. 11:1-44.9 provides penalties for violations of this subchapter.

The proposed new rules thus implement GLBA by requiring insurers and other licensees to develop appropriate standards and implement procedures to safeguard nonpublic information, while providing flexibility to those licensees to develop appropriate systems and programs commensurate with the sensitivity of the information, risk of disclosure of that information, potential harm of disclosure of that information, and the licensee's activities.

A 60-day comment period is provided for this notice of proposal, and, therefore, pursuant to N.J.A.C. 1:30-3.3(a)5, the proposal is not subject to the provisions of N.J.A.C. 1:30-3.1 and 3.2 governing rulemaking calendars.

Social Impact

As set forth in the Summary above, the proposed new rules implement the requirements of GLBA to require insurance licensees to safeguard information that is nonpublic under State or

Federal law. The proposed new rules therefore benefit the public by helping to protect the security, confidentiality and integrity of customer information, while providing licensees with flexibility to development appropriate systems and programs to safeguard this information, commensurate with the type of information involved, and the licensee's activities.

Economic Impact

Insurers, producers, and other licensees under Title 17 or 17B of the New Jersey Statutes will be required to bear any costs associated with developing systems and programs required pursuant to these rules. However, the Department notes that Federal law requires that these entities develop such programs to protect confidential customer information. Moreover, the proposed new rules provide licensees with flexibility to develop appropriate programs commensurate with their activities, the information they maintain, and the risk of disclosure of otherwise confidential information. Accordingly, the Department does not believe that the proposed new rules will impose an undue economic burden on insurers, producers or other applicable licensees.

Federal Standards Statement

Federal standards or requirements are not specifically applicable to entities subject to GLBA that are regulated by the Department. As noted in the Summary above, various Federal agencies have promulgated rules governing the entities they regulate. The requirements in these proposed new rules are generally comparable to the requirements imposed under those Federal rules.

Jobs Impact

The Department does not anticipate that any jobs will be generated or lost as a result of the proposed new rules. The proposed new rules require that licensees develop appropriate security programs to safeguard the confidentiality of nonpublic customer information under GLBA. The Department believes that the expertise for development of these programs will either be obtained in-house, or through consultants. The proposed new rules may increase the demand for the services of individuals or businesses with experience or expertise in developing programs as required under these proposed new rules.

The Department invites commenters to submit any data or studies concerning the jobs impact of the proposal together with their comments on other aspects of the proposal.

Agriculture Industry Impact

The proposed new rules will not have any impact on the agriculture industry in New Jersey.

Regulatory Flexibility Analysis

The proposed new rules may apply to "small businesses" as that term is defined in the Regulatory Flexibility Act, N.J.S.A. 52:14B-16 et seq. To the extent that the proposed new rules apply to small businesses, they will be insurers, agents, producers, insurance support organizations, and any person or entity that is subject to the statute governing information practices at N.J.S.A. 17:23A-1 et seq.

No new reporting requirements are imposed by these proposed rules. It is not anticipated that compliance with the recordkeeping requirements imposed by proposed N.J.A.C. 11:1-44.5(b) will necessitate the utilization of any professional services.

Entities subject to the proposed new rules will be required to implement a written information security program for safeguarding customer information. These entities will be required to bear any costs associated with developing and monitoring programs pursuant to these proposed new rules. In some instances, professional consultants or attorneys with expertise in privacy and confidentiality issues may need to be retained. Given the broad spectrum of licensees to which these proposed rules apply, initial and annual compliance costs are difficult to estimate. However, in developing the security program, the proposed new rules provide that the program shall be appropriate to the size and complexity of the licensee and the nature and scope of its activities. Accordingly, the proposed new rules provide flexibility for entities to develop appropriate plans for the protection and safeguarding of customer information as required by Federal law, consistent with the size of the entity.

Smart Growth Impact

The proposed new rules will not have an impact on the achievement of smart growth or the implementation of the State Development and Redevelopment Plan.

Full text of the proposed new rules follows:

SUBCHAPTER 44. STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

11:1-44.1 Purpose and scope

(a) This subchapter 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, 15 U.S.C. §§6801, 6805(b) and 6807.

(b) This subchapter shall apply to all licensees as defined herein.

(c) This subchapter shall not be deemed to limit or affect the duty of a licensee to maintain as confidential information required to be kept confidential pursuant to law, including, but not limited to, N.J.S.A. 17:23A-1et seq.

11:1-44.2 Definitions

The following words and terms, when used in this subchapter, shall have the following meanings, unless the context clearly indicates otherwise:

"Consumer" means an individual who seeks to obtain, obtains or has obtained an insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, and about whom the licensee has nonpublic personal information, or that individual's legal representative.

"Customer" means a consumer who has a customer relationship with a licensee.

"Customer information" means nonpublic personal information as defined in this section about a customer, whether in paper, electronic or other form, that is maintained by or on behalf of the licensee.

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

"Customer relationship" means a continuing relationship between a consumer and a licensee under which the licensee provides one or more insurance products or services to the consumer that are to be used primarily for personal, family or household purposes. A consumer has a continuing relationship with a licensee if:

1. The consumer is a current policyholder of an insurance product issued by or through the licensee; or

2. The consumer obtains financial, investment or economic advisory services relating to an insurance product or service from the licensee for a fee.

"Licensee" means all licensed insurers, producers and other persons licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to Titles 17 and 17B of the New Jersey Statutes, health maintenance organizations holding a certificate of authority pursuant to N.J.S.A. 26:2J-1 et seq., and any other person or entity subject to the statute governing information practices at N.J.S.A.17:23A-1 et seq.

"Licensee" shall not include: a purchasing group; or an unauthorized insurer in regard to the surplus lines business conducted pursuant to N.J.S.A. 17:22-6.40 et seq.

"Nonpublic personal information" means "personal information" and "privileged information" as defined in N.J.S.A.17:23A-2.

"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.

11:1-44.3 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.

11:1-44.4 Objectives of information security program

(a) 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.

11:1-44.5 Assess risk

(a) A licensee shall assess risk as set forth in (a)1 through 3 below. A licensee shall:

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

2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and

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

(b) A licensee shall maintain, for a period of not less than five years, records and documentation of the methodology utilized to assess risk, and the results of any deficiencies revealed from assessments performed pursuant to (a) above.

11:1-44.6 Manage and control risk

(a) A licensee shall manage and control risk as set forth in (a)1 through 3 below. A licensee shall:

1. 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;

2. Train staff, as appropriate, to implement the licensee's information security program; and

3. 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.

11:1-44.7 Service provider agreements

(a) A licensee shall oversee service provider agreements as (a)1 through 3 below. A licensee shall:

1. Exercise appropriate due diligence in selecting its service providers; and

2. Require its service providers to implement appropriate measures designed to meet the objectives of this subchapter, and, where indicated by the licensee's risk assessment, take appropriate steps to confirm that its service providers have satisfied these obligations.

11:1-44.8 Adjustment of the program

A licensee shall 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.

11:1-44.9 Violations

Failure to comply with the provisions of this subchapter, shall be deemed to constitute a violation of the statutes governing trade practices at N.J.S.A. 17:29B-1 et seq. and 17B:30-1 et seq., as applicable, and shall result in the imposition of penalties as provided in those statutes, N.J.S.A. 17:22A-1 et seq., 17:23A-1 et seq., 17:33-2, and any other provision of law.

jc02-10/inoregs