INSURANCE
DEPARTMENT OF BANKING AND INSURANCE
DIVISION OF INSURANCE

Standards for Safeguarding Customer Information

Reproposed 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 2003-455

Submit comments by January 16, 2004 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 of Banking and Insurance (Department) originally proposed new rules to implement that aspect of GLBA on March 3, 2003 at 35 N.J.R. 1186(a). Based on comments received, as set forth below, the Department has determined it is appropriate to repropose the rules to revise aspects regarding compliance, record retention, and a delayed effective date.

The Department is reproposing these rules with respect to insurers, producers and other licensees under Title 17 and 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 reproposed 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 reproposed 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 reproposed 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.

When the rules were originally proposed the Department received comments from the following:

1. The American Council of Life Insurers;
2. The American Insurance Association;
3. New Jersey Manufacturers Insurance Group;
4. Health Net of the Northeast, Inc.;
5. AmeriHealth Insurance Company of New Jersey and AmeriHealth HMO, Inc.;
6. The New Jersey Association of Mutual Insurance Companies;
7. Allstate New Jersey Insurance Company;
8. Horizon Blue Cross Blue Shield of New Jersey;
9. The Insurance Council of New Jersey;

10. The Health Insurance Association of America;

11. The Professional Insurance Agents of New Jersey;

12. The Independent Insurance Agents of New Jersey;

13. State Farm Insurance Companies;

14. The National Association of Independent Insurers;

15. The Alliance of American Insurers; and

16. Delta Dental Plan of New Jersey, Inc.

COMMENT: Virtually all of the commenters expressed concern that the rules as originally proposed, which were based on a model by the National Association of Insurance Commissioners (NAIC), made the requirements in N.J.A.C. 11:1-44.5 through 44.8 into mandates, whereas in the NAIC Model and in other states that have adopted the model, these provisions are utilized as examples to satisfy the requirements at N.J.A.C. 11:1-44.3 and 44.4. Several commenters noted that the NAIC Model provides that those examples are illustrative and not exclusive, while the proposed rule mandated that only those particular methods be used. The commenters believed that this would preclude licensees from developing actions and procedures that are workable for them, while meeting the objectives of the rule. One commenter specifically suggested that a new section at N.J.A.C. 11:1-44.5 be added as follows:

"11:1-44.5 Examples of Methods of Development and Implementation.

The actions and procedures described in sections 11:1-44.5, 44.6, 44.7 and 44.8 of this subchapter are examples of methods of implementation of the requirements of sections 11:1-44.3 and 44.4 of this subchapter. These examples are non-exclusive illustrations of actions and procedures that licensees may follow to implement sections 11:1-44.3 and 44.4 of this subchapter."

The commenter suggested that the existing N.J.A.C. 11:1-44.5 through 44.9 be recodified accordingly, and that the language mandating that licensees take action currently set forth in N.J.A.C. 11:1-44.5 through 44.8 be eliminated and that those provisions track the NAIC Model language.

RESPONSE: Upon review of the commenters' suggestions and concerns, the Department has determined that it is appropriate to revise the rules upon reproposal to reflect the approach set forth in the NAIC Model, which has been adopted by other states, including New York and California. The Department originally proposed the requirements as "mandates" in order to provide definitive guidance to licensees on what an acceptable "floor" would be with respect to taking actions to safeguard the confidentiality of information as required by law. The Department did not believe that the minimums set forth in the rules as originally proposed would impose an undue burden on licensees. However, the Department recognizes the desirability of maintaining a uniform regulatory structure implementing GLBA with respect to the safeguarding of confidential information, given the national scope of that statute. The Department believes that the reproposed rules will provide adequate protections and guidance to licensees with respect to maintaining and safeguarding confidential information pursuant to law, while providing licensees the flexibility to achieve that goal, consistent with the national standard adopted by the NAIC and other states.

COMMENT: Several commenters expressed concern with the record retention requirement set forth in N.J.A.C. 11:1-44.5(b) as originally proposed, which required that a licensee 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 risk assessments performed pursuant to that rule. The commenters generally stated that the five year record retention requirement was not contained in the NAIC model.

One commenter stated that the NAIC Market Conduct Record Retention Model Regulation requires that records be maintained for the current calendar year plus two calendar years. Another commenter stated that the rule would require licensees to keep information that is not normally kept as part of an insurer's record retention requirements. Another commenter stated that the rules should be adjusted to recognize that various information items are so fluid that a strict retention requirement is unnecessary. This commenter also stated that companies have already implemented record retention programs, and therefore there is no need to mandate the requirement here.

RESPONSE: The record retention requirement was intended to reflect the fact that insurers are subject to examination by the Department not less frequently than once every five years pursuant to N.J.S.A. 17:23-20 et seq. The purpose of this provision was to provide guidance to insurers and other licensees with respect to the time that records should be retained. The Department has received inquiries on numerous occasions with respect to record retention requirements. The Department historically has advised that licensees should maintain records as necessary to permit the Department to conduct an examination of their affairs and determine compliance with applicable law. The Department also notes that it has not adopted the NAIC Model Market Conduct Record Retention Regulation. Moreover, as noted by one of the commenters, the model Market Conduct Regulation essentially has a record retention requirement of three years. The Department does not believe that a retention requirement of five years is unduly burdensome or

significantly more onerous than the standard adopted by the NAIC referenced by one of the commenters. In any event, insofar as the rules as reproposed do not provide a mandate for the assessment of risk at N.J.A.C. 11:1-44.5 (recodified as 44.6), the Department has revised the rules to provide that licensees should maintain appropriate records to permit the Department to evaluate compliance with N.J.A.C. 11:1-44.3 and 44.4. This should provide additional flexibility for licensees while advising them they should maintain appropriate records for the Department to evaluate and determine their compliance with the rules.

COMMENT: Several commenters raised concerns with various definitions set forth in the rules.

One commenter stated that the rules rely on the existing 1982 Model definitions that sometimes conflict with those in the 2000 NAIC Model Privacy Regulation. The commenter stated that when the NAIC developed its model on this issue, it utilized the Model Privacy Regulation definitions as a guide. The commenter stated that utilization of the definitions as drafted will compromise an insurer's ability to comply with the rules and will render state-to-state operational uniformity on data security impossible. The commenter thus recommended that the definitions from the 2000 NAIC Model Privacy Regulation be utilized in this rule.

Another commenter stated that the rule either should provide a specific definition that references financial services to include products such as life, health, annuities, etc., or alternatively should modify the current definition of "customer relationship," which refers to "services," to include the foregoing services. The commenter believed that the current definition of "customer relationship" is subject to multiple interpretations.

Another commenter stated that the definition of "consumer" does not need to include an individual who seeks to obtain an insurance product or service since the rules do not apply with respect to these persons. The commenter stated that the requirements of the rule apply only to customers and customer information. The rule would not apply to an individual who merely applies for insurance.

RESPONSE: Upon review of the commenters' concerns, the Department has determined that no changes are required. With respect to definitions that may deviate from the 2000 NAIC Model Privacy Regulation, the Department notes that New Jersey has not adopted the 2000 Model Privacy Regulation. Rather, the existing statute, at N.J.S.A. 17:23A-1 et seq., is based on the 1982 NAIC Model law. The Department believes that it is reasonable, appropriate, and in fact required, to utilize definitions set forth in New Jersey law where they exist. The Department does not believe that this will render it "impossible" for insurers to comply with the rules. Indeed, the requirements regarding insurer information practices at N.J.S.A. 17:23A-1 et seq., which sets forth the information insurers must maintain as confidential and limits the release of certain information, may vary between states that utilize the 1982 Model Information Practices Act, such as New Jersey, and states that adopt the 2000 NAIC Model Privacy Regulation, in order to comply with requirements under GLBA.

With respect to the concerns regarding the definition of "customer relationship," the Department notes that this definition is based on the NAIC Privacy of Consumer Financial and Health Information Regulation. In order to provide further clarification and guidance, the Department has included in the reproposal additional examples of what does not constitute a "customer relationship" that tracks the above-referenced NAIC Model.

Finally, with respect to questions as to why a definition of "consumer" is included, this definition is provided because it is referenced in other definitions in the rules. Moreover, the definition of "consumer" is based on the NAIC Model Privacy Consumer Financial and Health Information Regulation. Accordingly, the Department believes that the definitions utilized are appropriate and reflect the NAIC Model standards.

COMMENT: Several commenters expressed concern with N.J.A.C. 11:1-44.9, which provides that failure to comply with these rules 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. One commenter stated that the rules should make clear that enforcement under the rules would not trigger the limited private right of action set forth in the New Jersey Information Practices Act. In addition, the commenter stated that penalties should apply only to willful or intentional violations, or a pattern or practice of misbehavior, not to minor violations. The commenter further believed that the Department should be given discretion to apply a penalty, which will ensure that severe penalties will not be imposed for inadvertent violations and that the Department will retain the authority to decide whether violations require sanctions at all. Another commenter believed that the provisions should be removed because it would invite private causes of action.

RESPONSE: Upon review, the Department has determined not to change this provision. The penalties provision is consistent with the national standard as reflected in the NAIC Model, and has been adopted in several states, including New York and California. As currently provided under applicable law, the Department would retain appropriate discretion as to whether to impose penalties. In addition, the Department does not believe that the rules should limit the

ability of the Department to impose sanctions solely to patterns of misconduct or willful or knowing violations of the rules. It may be difficult or impossible to ascertain whether a violation was knowing or willful. Furthermore, an egregious violation of applicable law, even though it may not be knowing or willful, may appropriately be subject to sanction by the Department. The Department also does not believe that it is necessary to state that violations of this subchapter may not be enforced by a private cause of action. The rights of private parties are appropriately set forth in applicable statutes and case law.

COMMENT: Several commenters requested that the rules provide a delayed effective date for implementation. One commenter requested that, given the broad definition of "service providers," compliance with N.J.A.C. 11:1-44.7 pertaining to service provider agreements is onerous, and recommended that the effective date for all new service provider agreements be upon adoption, but delayed for one year on any existing service provider agreements. The commenter stated that this approach was utilized when GLBA was implemented.

Two commenters stated that covered entities must comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) by April 21, 2005. To avoid duplication of efforts by a licensee to meet different state and Federal security standards, the commenter suggested that the effective date of compliance with these rules be consistent with the Federal compliance date of April 21, 2005. Another commenter suggested that an effective date of April 14, 2004 be utilized, which this commenter stated was the effective date of the HIPAA privacy rule compliance.

Another commenter suggested an effective date of 30 days after rule adoption. Two commenters suggested a delayed effective date of six months, and one of these commenters

suggested that a new rule at N.J.A.C. 11:1-44.11 be provided which sets forth an implementation date as follows: "Each licensee shall establish and implement an information security program, including appropriate policies and systems pursuant to this regulation, on or before six months after the effective date of these regulations."

RESPONSE: The Department believes that it is reasonable and appropriate to provide for a delayed effective date for licensees to comply with these rules. Given the broad nature of these rules as reproposed, which provide no specific mandates other than each licensee shall implement a security program, the Department believes that an effective date of six months should provide sufficient time for licensees to develop systems to comply with these rules. The Department notes that licensees already have been required to comply with similar rules in New York since June 1, 2002, and as a result of enactment of GLBA, have been aware of the potential for these requirements since before that time. In addition, the original rules were proposed on March 3, 2003. Accordingly, the Department believes that insurers have been provided ample time to begin to develop systems necessary to comply with this subchapter.

COMMENT: Several commenters believed that there was a typo in N.J.A.C. 11:1-44.7(a), which referred to three requirements, where there were only two requirements listed.

RESPONSE: The proposal as published in the New Jersey Register and as reproposed does not contain the stated typographical error.

COMMENT: One commenter stated it was unclear what the term "service provider" at N.J.A.C. 11:1-44.2 means. The commenter stated that it believed it referred to entities and persons who manage a designated record set on behalf of the health plan as a result of the service they provide to the health plan or functionally perform on behalf of the health plan. Alternatively, the commenter stated that if the Department is referring to health care providers who provide services to the members of a health plan, a health plan is not able to control, oversee, or require any activity of an out-of-network provider, including the provider's privacy and security measures.

RESPONSE: The Department believes that the definition is clear and refers to a person who provides services "directly to the licensee." If a service provider is permitted access to customer information, the licensee may need to consider whether it should, through its contract, require the service provider to implement measures to meet the objectives of the rule, as set forth at N.J.A.C. 11:1-44.9.

COMMENT: One commenter stated that it appears that compliance with these proposed standards may be duplicative of the requirements under HIPAA. Therefore, the commenter proposed that a new section be provided to read as follows: "A licensee's compliance with the administrative, technical and physical safeguard standards set forth in section 164.530 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy rule, shall be deemed compliance with the subchapter."

RESPONSE: Although the Department anticipates that development of appropriate programs under HIPAA would comply with the requirements set forth under these rules as required by GLBA, the Department disagrees that a change is required. While it is true that insurers or other licensees may be required to develop similar programs in order to comply with HIPAA and the requirements for safeguarding customer information under GLBA, the Department does not believe it is appropriate to codify by rule that compliance with Federal HIPAA rules shall, as a matter of law, be deemed compliance with New Jersey requirements. The Department notes that these rules as drafted provide broad guidance as to how a licensee may comply.

COMMENT: One commenter questioned whether there is any specific "nonpublic personal information" that does not fall under the definition of either "personal information" or "privileged information" as defined in N.J.S.A. 17:22A-2 that also should be protected. The commenter cited the following as examples: social security number; telephone number; drivers license; location of home, if not the mailing address; name of employer; place of employment; and dependent information. The commenter believed that if the Department determines that there are additional items of nonpublic personal information that should be protected, they should be included in the rule.

RESPONSE: Upon review, the Department has determined that no change is required. The Department believes that the rules appropriately provide guidance to licensees as to the information currently required to be confidential under New Jersey law. Licensees may develop systems to safeguard information required to be kept confidential under Federal law or law other

than New Jersey insurance law. The Department will monitor this issue, and to the extent it believes additional guidance is necessary, will propose amendments to the rules at that time.

COMMENT: One commenter requested the Department clarify the rule with respect to the responsibilities for independent insurance agents. The commenter noted that under the rules, agents would be required to add a written technology privacy standard policy, perform additional training and auditing, and keep auditing records that could be reviewed by the Department.

RESPONSE: The Department believes that the rules as revised upon reproposal set forth the requirements, as ultimately mandated by GLBA, that licensees, which include independent insurance agents, implement an information security program as required under N.J.A.C. 11:1-44.3.

COMMENT: One commenter stated that the term "appropriate" in N.J.A.C. 11:1-44.3 means "reasonable" and "scalable" and suggested that the Department utilize those descriptives. In addition, the commenter stated that under N.J.A.C. 11:1-44.4, the rule requires that a licensee's information security program should be designed to "ensure" the security and confidentiality of customer information. The commenter stated that "ensure" could be interpreted to mean "make certain" which may not be feasible. The commenter requested that the Department change the language to read "a licensee's information security program shall be designed to take reasonable steps to..." or that "a licensee's information security program shall reasonably …." (underlined language is to be added)

RESPONSE: Upon review, the Department has determined not to change these provisions. These provisions are based on the NAIC Model and reflect the national standard adopted by states that have adopted the model thus far, including New York and California. Moreover, Section 501(b) of GLBA requires each agency to establish appropriate standards for financial institutions relating to administrative, technical and physical safeguards, *inter alia*, to **ensure** the security and confidentiality of customer records and information (emphasis supplied). Accordingly, the language in the NAIC model and in the rules as reproposed, reflect the language set forth under GLBA.

A summary of the reproposed new rules follows:

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 such 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 provides that the actions and procedures described in N.J.A.C. 11:1-44.6 through 44.9 are examples of methods of implementation of the requirements in N.J.A.C. 11:1-44.3 and 44.4, and are non-exclusive.

Proposed N.J.A.C. 11:1-44.6 describes that licensees may assess the risk of threats to the confidentiality of information.

Proposed N.J.A.C. 11:1-44.7 describes that a licensee may 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 testing or otherwise monitoring key controls, systems and procedures of the security program.

Proposed N.J.A.C. 11:1-44.8 provides that a licensee may 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. 11:1-44.9 describes that a licensee may 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. 11:1-44.10 provides penalties for violations of this subchapter.

Proposed N.J.A.C. 11:1-44.11 sets forth the effective date for compliance with the rules.

The reproposed 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 the information, potential harm from 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 reproposed new rules implement the requirements of GLBA to require insurance licensees 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 develop 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 reproposed 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 reproposed 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

reproposed 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 reproposed new rules. The reproposed 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 reproposed new rules may increase the demand for the services of individuals or businesses with experience or expertise in developing programs as required under these reproposed 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 reproposed new rules will not have any impact on the agriculture industry in New Jersey.

## Regulatory Flexibility Analysis

The reproposed new rules will 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 reproposed 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 reproposed rules.

Entities subject to the reproposed 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 reproposed 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 reproposed 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 reproposed 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 the confidentiality of 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.

1. A consumer has a continuing relationship with a licensee if:

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

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

2. A consumer does not have a continuing relationship with a licensee if:

i. The consumer applies for insurance but does not purchase the insurance;

ii. The licensee sells the consumer airline travel insurance in an isolated transaction;

iii. The individual is no longer a current policyholder of an insurance product or no longer obtains insurance services with or through the licensee;

iv. The consumer is a beneficiary or claimant under a policy and has submitted a claim under a policy choosing a settlement option involving an ongoing relationship with the licensee;

v. The consumer is a beneficiary or a claimant under a policy and has submitted a claim under that policy choosing a lump sum settlement option;

vi. The customer's policy lapsed, expired or otherwise became inactive or dormant under the licensee's business practices, and the licensee has not communicated with the

customer about the relationship for a period of 12 consecutive months, except through annual privacy notices, material distributions or mass mailings required by law or regulation, communication at the direction of a state or Federal authority, or promotional materials;

vii. The individual is an insured or an annuitant under an insurance policy or annuity, respectively, but is not the policyholder or owner of the insurance policy or annuity; or

viii. The individual's last known address of record is deemed invalid for the purposes of this subchapter. An address of record is deemed invalid if mail sent to that address by the licensee has been returned by the postal authorities as undeliverable and if subsequent attempts by the licensee to obtain a current valid address for the individual have been unsuccessful.

"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-2t and w, respectively.

"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

(a) 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.

(b) A licensee shall maintain and make available appropriate records to enable the Department to determine compliance with the requirements of this subchapter.

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 customer information; and

3. Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.

11:1-44.5 Examples of methods of development and implementation

The actions and procedures described in N.J.A.C. 11:1-44.6 through 44.9 are examples of methods of implementation of the requirements of N.J.A.C. 11:1-44.3 and 44.4. These examples are non-exclusive illustrations of actions and procedures that licensees may follow to implement N.J.A.C. 11:1-44.3 and 44.4.

11:1-44.6 Assessment of risk

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

11:1-44.7 Management and control of risk

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

11:1-44.8 Service provider agreements

The licensee exercises appropriate due diligence in selecting its service providers; and requires its service providers to implement appropriate measures designed to meet the objectives of this subchapter, and, where indicated by the licensee's risk assessment, takes appropriate steps to confirm that its service providers have satisfied these obligations.

11:1-44.9 Adjustment of 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.

11:1-44.10 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.

11:1-44.11 Effective date

A licensee shall establish and implement an information security program, including appropriate policies and systems pursuant to this subchapter, by (six months from the effective date of this subchapter).

jc03-47a/inoregs