114CSR62

WEST VIRGINIA LEGISLATIVE RULE

INSURANCE COMMISSIONER

SERIES 62

STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

Section.

114CSR62

WEST VIRGINIA LEGISLATIVE RULE

INSURANCE COMMISSIONER

SERIES 62

STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

§114-62-1. General.

1.1. Scope. -- This rule 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 and 507, and subsection 505(b) of the Gramm-Leach-Bliley Act, codified at 15 U.S.C. 6801, 6807 and 6805(b). Section 507 of the Act provides, among other things, that a state regulation may afford persons greater privacy protections than those provided by subtitle A of Title V of the Gramm-Leach-Bliley Act. The safeguards established pursuant to this rule shall apply to nonpublic personal information, including nonpublic personal financial information and nonpublic personal health information.

1.2. Authority. -- W.Va. Code §§33-6F-1 and 33-2-10.

a. Subsection 501(a) of the Gramm-Leach-Bliley Act, 15 U.S.C. 6801, 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.

b. Subsection 501(b) of the Act requires the state insurance regulatory authorities to 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. Paragraph 505(b)(2) of the Gramm-Leach-Bliley Act, 15 U.S.C. 6805(b), calls on state insurance regulatory authorities to implement the standards prescribed under subsection 501(b) by regulation with respect to persons engaged in providing insurance.

d. Paragraph 503(a)(3) of the Gramm-Leach-Bliley Act, codified at 15 U.S.C. section 6803(a)(3), requires each financial institution to develop policies for protecting the nonpublic personal information of consumers and to make those policies available in written form.

1.3. Filing Date. -- April 3, 2003.

1.4. Effective Date. -- April 3, 2003.

§114-62-2. Definitions.

2.1. “Customer” means a customer of the licensee as the term is defined in subsection 2.9 of the insurance commissioner's rule on privacy of consumer financial and health information, 114CSR57.

2.2. “Customer information” means any nonpublic personal information as defined in subsection 2.19 of the insurance commissioner's rule on privacy of consumer financial and health information, 114CSR57, about a customer, whether in paper, electronic or other form, that is maintained by or on behalf of the licensee. For purposes of this rule, customer information shall also include information submitted to a licensee by a

consumer on an application for an insurance product, regardless of whether the insurance product is ultimately purchased by the consumer.

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

2.4. “Licensee” means a licensee as that term is defined in subsection 2.17 of the insurance commissioner's rule on privacy of consumer financial and health information, 114CSR57, except that “licensee” shall not include:

a. A purchasing group; or

b. An unauthorized insurer in regard to the excess line business conducted pursuant to article twelve-c, chapter thirty-three of the West Virginia Code.

2.5. “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.

§114-62-3. Information Security Program.

3.1. 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.

§114-62-4. Objectives of Information Security Program.

4.1. 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.

§114-62-5. Methods of Development and Implementation.

5.1. The actions and procedures set forth in this section are nonexclusive examples of methods a licensee may use to implement the requirements of sections three and four of this rule.

5.2. The licensee assesses risk by:

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

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

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

5.3. The licensee manages and controls risk by:

a. Designing its information security program to control the identified risks, commensurate with the sensitivity of the information and the complexity and scope of the licensee's activities;

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

c. Regularly testing or otherwise regularly monitoring the key controls, systems and procedures of the information security program. The frequency and nature of these tests or other monitoring practices shall be determined by the licensee's risk assessment.

5.4. The licensee oversees service provider arrangements by:

a. Exercising appropriate due diligence in selecting its service providers; and

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

5.5. The licensee monitors, evaluates and adjusts, as appropriate, its 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.

§114-62-6. Violation.

6.1 Violations of this rule are subject to the provisions of W. Va. Code §§33-3-11 and 33-12-24.