WEST VIRGINIA
SECRETARY OF STATE
JOE MANCHIN, III
ADMINISTRATIVE LAW DIVISION

Form #2

Do Not Mark In This Box

FILED

2002 MAY 29 P 2:31

OFFICE WEST VIRGINIA
SECRETARY OF STATE

NOTICE OF A COMMENT PERIOD ON A PROPOSED RULE

AGENCY: Insurance Commissioner TITLE NUMBER: 114

RULE TYPE: Legislative CITE AUTHORITY: W. Va. Code §§ 33-2-10 and 33-6F-1

AMENDMENT TO AN EXISTING RULE: YES ____ NO X

IF YES, SERIES NUMBER OF RULE BEING AMENDED: ____

TITLE OF RULE BEING AMENDED: ____

IF NO, SERIES NUMBER OF RULE BEING PROPOSED: 62

TITLE OF RULE BEING PROPOSED: Standards for Safeguarding Consumer Information

IN LIEU OF A PUBLIC HEARING, A COMMENT PERIOD HAS BEEN ESTABLISHED DURING WHICH ANY INTERESTED PERSON MAY SEND COMMENTS CONCERNING THESE PROPOSED RULES. THIS COMMENT PERIOD WILL END ON July 1, 2002 AT 4:30 p.m. ONLY WRITTEN COMMENTS WILL BE ACCEPTED AND ARE TO BE MAILED TO THE FOLLOWING ADDRESS:

Mary Jane Pickens, Associate Counsel

West Virginia Insurance Commission
P.O. Box 50540

Charleston, WV 25305-0540

THE ISSUES TO BE HEARD SHALL BE LIMITED TO THIS PROPOSED RULE.

Brian Lastinger

Authorized Signature

ATTACH A **BRIEF** SUMMARY OF YOUR PROPOSAL

SCANNED

$4.40

Department of Tax and Revenue
Agency Questionnaire

Re: Legislative Rule to be Filed

STANDARDS FOR SAFEGUARDING CONSUMER INFORMATION

TITLE 114, SERIES 62

Question 1: Are regulations required?

Yes, subsection 501(b) of the Gramm-Leach-Bliley Act, 15 U.S.C. 6801, requires the state insurance regulatory authorities, with respect to persons engaged in providing insurance, to establish appropriate standards relating to administrative, technical and physical safeguards to ensure the security and confidentiality of customer records and information; to protect against any anticipated threats or hazards to the security or integrity of such records; and to protect against unauthorized access to or use of records or information that could result in substantial harm or inconvenience to a customer.

Question 2: Is the rule you are proposing controversial? If yes, what are the pros and the cons?

The Legislature passed the Insurance Commissioner's rule on Privacy of Consumer Financial and Health Information, 114CR57, during the regular 2002 Legislative Session. The privacy concepts set forth in this rule are by now well known in the insurance industry as a result of the promulgation of the rule on Privacy of Consumer Financial and Health Information. The model NAIC Rule generally uses the term "customer" where "consumer" is used in this proposed rule, and comments may be received on this point. However, the Gramm-Leach-Bliley Act clearly requires the protection of non-public personal information of consumers and customers, and there was concern when proposing this rule that insurers may fail to properly implement its measures as to consumer information. Therefore, where "customer" appears in the model rule, the word "consumer" appears in this proposed rule.

Question 3: Is the rule you are proposing a copy of another state's rule? A model rule? Custom-drafted?

The rule is a model regulation passed by the National Association of Insurance Commissioners ("NAIC") on April 10, 2002.

Question 4: What are the really important things you think the Secretary of Tax and Revenue should know about this rule and the issues that surround it?

This rule establishes standards for developing and implementing administrative, technical and physical safeguards to protect the security, confidentiality and integrity of consumer and 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, 6805(b) and 6807. 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. Subsection 503(a) of the act requires each financial institution to develop policies for protecting the non-public personal information of consumers and to make those policies available in written form. Subsection 501(b) of the act requires the state insurance regulatory authorities, with respect to persons engaged in providing insurance, to establish appropriate standards relating to administrative, technical and physical safeguards to ensure the security and confidentiality of customer records and information; to protect against any anticipated threats or hazards to the security or integrity of such records; and to protect against unauthorized access to or use of records or information that could result in substantial harm or inconvenience to a customer. This rule will bring the state into compliance with these directives.

Insurance Commissioner
Legislative Rule
Title 114, Series 62

STANDARDS FOR SAFEGUARDING CONSUMER INFORMATION

TITLE 114, SERIES 62

BRIEF SUMMARY OF RULE

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. This rule, which was adopted by the National Association of Insurance Commissioners as a model regulation on April 10, 2002, 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, 6805(b) and 6807. Subsection 501(b) of the act requires the state insurance regulatory authorities, with respect to persons engaged in providing insurance, to establish appropriate standards relating to administrative, technical and physical safeguards to ensure the security and confidentiality of customer records and information; to protect against any anticipated threats or hazards to the security or integrity of such records; and to protect against unauthorized access to or use of records or information that could result in substantial harm or inconvenience to a customer. This rule will bring the state into compliance with these directives.

Insurance Commissioner
Legislative Rule
Title 114, Series 62

STANDARDS FOR SAFEGUARDING CONSUMER INFORMATION

TITLE 114, SERIES 62

STATEMENT OF CIRCUMSTANCES

On April 10, 2002, the National Association of Insurance Commissioners ("NAIC") adopted the Standards for Safeguarding Customer Information Model Regulation, and urged all states to immediately promulgate the model as a rule. 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, 6805(b) and 6807. 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. Subsection 503(a) of the act requires each financial institution to develop policies for protecting the non-public personal information of consumers and to make those policies available in written form. Subsection 501(b) of the act requires the state insurance regulatory authorities, with respect to persons engaged in providing insurance, to establish appropriate standards relating to administrative, technical and physical safeguards to ensure the security and confidentiality of customer records and information; to protect against any anticipated threats or hazards to the security or integrity of such records; and to protect against unauthorized access to or use of records or information that could result in substantial harm or inconvenience to a customer. This rule will bring the state into compliance with these directives.

APPENDIX B

FISCAL NOTE FOR PROPOSED RULES

Rule Title: Standards for Safeguarding Consumer Information
Title 114, Series 62

Type of Rule: __X__ **Legislative** ___**Interpretive** ____**Procedural**

Agency: Insurance Commissioner

Address: Post Office Box 50540
1124 Smith Street, Greenbrooke Building
Charleston, West Virginia 25305-0540

==========

1. Effect of Proposed Rule

	ANNUAL		FISCAL YEAR		
	Increase	Decrease	Current	Next	Thereafter
ESTIMATED TOTAL COST	None	None	None	None	None
PERSONAL SERVICES	None	None	None	None	None
CURRENT EXPENSE	None	None	None	None	None
REPAIRS AND ALTERNATIONS	None	None	None	None	None
EQUIPMENT	None	None	None	None	None
OTHER	None	None	None	None	None

2. Explanation of above estimates:

The rule will have no additional fiscal impact upon state, local or federal government.

3. Objectives of these rules:

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. The objective of this rule,

is to establish 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, 6805(b) and 6807.

4. Explanation of Overall Economic Impact of Proposed Rule.

A. Economic Impact on State Government.

None

B. Economic Impact on Political Subdivisions; Specific Industries; Specific groups of Citizens.

This rule will establish standards for developing and implementing administrative, technical and physical safeguards to protect the security, confidentiality and integrity of consumer and customer information. The rule will have an economic impact on licensees subject to the rule and subject to the Insurance Commissioner's rule on Privacy of Consumer Financial and Health Information. Licensees will be required to undertake steps to implement the protections, which may include such things as identifying risks or threats to the security of consumer information, designing an information security program to control those risks, staff training, regular monitoring of the program, and changes in methods of selecting and monitoring service providers. There will be costs involved with compliance by licensees. There should be no economic impact on political subdivisions or any specific groups of citizens.

C. Economic Impact on Citizens/Public at Large.

There is no anticipated economic impact on citizens or the public at large as a result of the promulgation of this rule.

Date: May 29, 2002

Signature of Agency Head or Authorized Representative

Mary Jane Pickens

MARY JANE PICKENS, ASSOCIATE COUNSEL

114CSR62
WEST VIRGINIA LEGISLATIVE RULE
INSURANCE COMMISSIONER

SERIES 62
STANDARDS FOR SAFEGUARDING CONSUMER INFORMATION

Section

114CSR62
WEST VIRGINIA LEGISLATIVE RULE
INSURANCE COMMISSIONER

SERIES 62
STANDARDS FOR SAFEGUARDING CONSUMER 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 consumer 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. This rule requires that 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. Paragaph 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 non-public personal information of consumers and to make those policies available in written form.

1.3. Filing Date. --

1.4. Effective Date. --

§114-62-2. Definitions.

2.1. "Consumer" means a consumer of the licensee as the term consumer is defined in subsection 2.6 of the insurance commissioner's rule on privacy of consumer financial and health information, 114CSR57.

2.2. "Consumer 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 consumer, whether in paper, electronic or other form, that is maintained by or on behalf of the licensee.

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

3.2. If a licensee is domiciled in another jurisdiction and the statutes and regulations

administered by its domiciliary regulator establish standards for protecting the security of consumer information which are substantially similar to those established by this rule, then good faith compliance with those standards to the satisfaction of the licensee's primary regulator shall constitute compliance with this rule. A law shall not be considered dissimilar because it references "customers" rather than "consumers," as long as the licensee is not implementing its information security program in a manner that causes demonstrable harm to consumers who are not present or former customers.

§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 consumer 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 consumer.

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

5.1. The actions and procedures set forth in this section are examples of methods a licensee may use to implement the requirements of sections three and four of this rule. They are non-exclusive, and a licensee may use other methods of implementation if they will provide the same level of security and confidentiality of consumer information as the examples in this section.

5.2 The licensee shall assess risk by:

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

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

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

5.3. The licensee shall manage and control 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 shall oversee 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 shall monitor, evaluate and adjust, as appropriate, its information security program in light of any relevant changes in technology, the sensitivity of its consumer 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 consumer information systems.

§114-62-6. Violation.

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