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

Form #3

Do Not Mark In This Box

NOTICE OF AGENCY APPROVAL OF A PROPOSED RULE
AND
FILING WITH THE LEGISLATIVE RULE-MAKING REVIEW COMMITTEE

AGENCY: Insurance Commission TITLE NUMBER: 114

CITE AUTHORITY: West Virginia Code Sections 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 Customer Information

THE ABOVE PROPOSED LEGISLATIVE RULE HAVING GONE TO A PUBLIC HEARING OR A PUBLIC COMMENT PERIOD IS HEREBY APPROVED BY THE PROMULGATING AGENCY FOR FILING WITH THE SECRETARY OF STATE AND THE LEGISLATIVE RULE-MAKING REVIEW COMMITTEE FOR THEIR REVIEW.

Authorized Signature

QUESTIONNAIRE

(Please include a copy of this form with each filing of your rule: Notice of Public Hearing or Comment Period, Proposed Rule, and if needed, Emergency and Modified Rule.)

DATE: July 26, 2002

TO: LEGISLATIVE RULE-MAKING REVIEW COMMITTEE

FROM: OFFICE OF THE INSURANCE COMMISSIONER
ATTN: Legal Division
1124 Smith Street
Post Office Box 50540
Charleston, West Virginia 25305-0540

LEGISLATIVE RULE TITLE: STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION (Title 114, Series 62)

1. **Authorizing statute(s) citation:**

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

2. a. **Date filed in State Register with Notice of Hearing or Public Comment Period:**

      May 29, 2002 - Comment Period.

   b. **What other notice, including advertising, did you give of the hearing?**

      None

   c. **Date of Public Hearing(s) or Public Comment Period ended:**

      Comment period ended July 1, 2002.

   d. **Attach list of persons who appeared at hearing, comments received, amendments, reasons for amendments.**

      Attached ___X___ **No comments received** _____

   e. **Date you filed in State Register the agency approved proposed Legislative Rule following public hearing: (be exact)**

      July 26, 2002

f. Name, title, address and phone/fax/e-mail numbers of agency person(s) to receive all *written correspondence* regarding this rule: (Please type)

Mary Jane Pickens, Associate Counsel
West Virginia Insurance Commission
Legal Division
P.O. Box 50540
Charleston, WV 25305-0540
Phone: (304) 558-0401, ext. 159

Fax: (304) 558-1362
E-mail: pickensm@mail.wvnet.edu

g. IF DIFFERENT FROM ITEM 'f', please give Name, title, address and phone number(s) of agency person(s) who wrote and/or has responsibility for the contents of this rule: (Please type)

Not applicable

3. If the statute under which you promulgated the submitted rules requires certain findings and determinations to be made as a condition precedent to their promulgation:

a. Give the date upon which you filed in the State Register a notice of the time and place of a hearing for the taking of evidence and a general description of the issues to be decided.

Not applicable

b. Date of hearing or comment period:

Not applicable

c. On what date did you file in the State Register the findings and determinations required together with the reasons therefor?

Not applicable

d. Attach findings and determinations and reasons:

Not applicable

Insurance Commissioner
Title 114, Series 62

ATTACHMENT TO QUESTION 2(d):

Two sets of comments were received during the comment period in response to the proposed legislative rule; one from Alliance of American Insurers ("Alliance") and one from the American Insurance Association ("AIA").

A. Alliance of American Insurers ("Alliance")

1. Alliance comments on the scope of the rule and the proposed application of the rule to "consumer" information rather than "customer" information. Specifically, Alliance comments:

- The Gramm-Leach-Bliley Act requires this proposed rule to be narrowly limited to customers, not broadly applied to consumers also.

- The proposed rule will apply to a broader spectrum of information than other states' rules, making West Virginia a less attractive market for multi-state insurers and will impose additional expenses to create a special program just for West Virginia. Alliance states that this will translate into fewer choices for insurance consumers in this state and higher premiums for insureds.

- "Consumers" includes claimants and declined applicants. Third party claimants are already treated differently in the Unfair Trade Practices Act than policyholders, with whom the licensee has a contractual relationship.

- There should be a different level of safeguarding applicable to a customer, as opposed to a consumer, and Alliance members want to be able to decide for themselves what that level of safeguarding will be.

- The relationship between licensees and third party claimants is adversarial, and what little information insurers have about these consumers is often spread out in branch offices, or held by adjusters, investigators or attorneys. Alliance states that this is especially true in cases involving independent adjusters.

- Banks and securities firms are subject only to customer information regulations in place at the federal level. Therefore insurers would be at a competitive disadvantage if they have to protect consumer information as well as customer information.

In response to these comments from Alliance concerning the scope of the rule, the Commissioner points out that the Insurance Commission rule on Privacy of Consumer Financial and Health Information, 114CSR57, promulgated to allow regulation of insurers as it relates to the privacy provisions of the Gramm-Leach-Bliley Act, provides protection for consumers and customers. In other words, purchasing the product is not a prerequisite to enjoying the protections of Series 57. In fact, third party claimants, beneficiaries, and others are considered consumers of the licensee and entitled to notice and an opportunity to opt out of a disclosure under Series 57 if the licensee discloses protected information about such individuals outside of the exceptions in the rule.

Furthermore, paragraph 503(a)(3) of the Gramm-Leach-Bliley Act requires each financial institution to develop policies for protecting the nonpublic personal information of *consumers*, and to make those policies available in a written form. (emphasis added) This provision appears to express congressional intent of protecting the information of consumers. Although the proposed rule is intended to implement the specific provisions of subsection 501(b) of the Act, there is no discernable reason why Congress intended the term "customer" as it is used in subsection 501(b) to be a limiting term.

Another reason that application of the rule to consumer information should not be an onerous burden is that Series 57 only requires a privacy notice to be sent to consumers if the licensee plans to disclose a consumer's protected information outside of the exceptions in the rule. Therefore, it would appear that licensees should be trying to protect consumer information to avoid noncompliance with Series 57, unless they intend to send privacy and opt out notices to them. If a licensee has not sent a privacy notice and opt out to a consumer, it must be because it has no plans to disclose the consumer's information and therefore it is difficult to understand why the licensee would not also be taking appropriate measures to ensure the safety and integrity of that information.

In spite of the reasons set forth above, the Commissioner proposes a compromise on the scope of the proposed rule's application that would limit it to customer information, which will include, for purposes of the rule, applications for insurance products submitted by consumers regardless of the fact that the consumer does not actually purchase the product. Applications can contain a wealth of information, and the rule should protect that information even though the consumer does not establish a continuing relationship with the licensee. The Commissioner feels that the information in applications is clearly protected under Series 57, and should be subject to the physical and technical protections set forth in this proposed rule as well. The Commissioner therefore agrees to change all references to "consumer" in the rule to "customer," but to rewrite subsection 2.2 as follows:

> *"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 applications for an insurance product submitted to a licensee by a consumer, regardless of whether the insurance product is ultimately purchased by the consumer.*

The Commissioner further notes that subsection 3.2 had been included in the proposed rule to ease the burden of compliance with different rule requirements between different jurisdictions, in recognition that the rule as originally proposed required data security standards for a larger type of information than may be required by other states. Due to the change of focus of the proposed rule from "consumer" information to "customer" information (with the exception of applications submitted by consumers, as noted above), subsection 3.2 will no longer be necessary, and the Commissioner will delete the subsection from the proposed rule.

In further response to the comments of Alliance regarding the scope of the proposed rule, the Commissioner points out that state regulation may afford persons greater privacy protections than those provided by subtitle A of Title V of the Gramm-Leach-Bliley Act, pursuant to section 507 of the Act. The Commissioner disagrees that licensees should be able to choose for themselves whether to protect the information that consumers submit to them on an insurance application, or whether to disregard these protections so that the information could possibly end up on a website or otherwise displayed to the public. Gramm-Leach-Bliley allows this rule to provide protections for the kind of information set forth in applications submitted by consumers and the Commissioner believes that the scope of this rule should include this particular consumer information. The Commissioner further responds by saying that, although Alliance has offered no real evidence other than broad statements that application of the rule to consumer information will be substantially more costly for insurers, will result in higher premiums for insureds, or create an unfair competitive atmosphere with banks, the above compromise regarding the scope of the rule will not impose an undue burden or competitive disadvantage on licensees and addresses the comments from Alliance in this regard.

2. Alliance comments that the proposed rule imposes no specific time for compliance, and that analogous federal regulations provide 2 years to comply as to service provider contracts in effect prior to the date of the regulation. Alliance does not insist on 2 years, but suggests 6 months to comply as to service providers. A longer time to comply is needed as well if the rule is to apply to consumers as opposed to customers.

The Commissioner agrees that the rule contains no time for compliance, but points out that the rule was filed both as an emergency rule and as a legislative rule on May 29, 2002. The emergency rule became effective on July 3, 2002. The Commissioner agrees to amend the emergency rule to rewrite subsection 3.1 as follows (no change will be made to the legislative rule):

> *By February 1, 2003, 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.*

When the Legislature authorizes promulgation of the legislative rule, the emergency rule will be replaced. By that time, licensees should be in compliance.

B. American Insurance Association ("AIA")

1. AIA also comments on the scope of the proposed rule and the application of the rule to "consumer" information rather than "customer" information. Specifically, AIA comments as follows:

- The use of the word "consumer" runs counter to scope of the NAIC model and other jurisdictions proposing this model rule.
- The Gramm-Leach-Bliley Act's security standards focus on protecting only customer information.
- "Consumers" include third party claimants and others with whom licensees have no continuing business relationship.
- Expansion of the rule to consumers threatens uniformity across jurisdictional lines. This uniformity is needed to aid compliance implementation, reduce compliance costs, and level the competitive playing field. As proposed, the rule would require licensees to implement standards to safeguard more information than banks are required to safeguard under federal standards.
- Application of the rule to "consumers" goes beyond W.Va. Code §33-6F-1, which is the statutory authority for promulgating the rule. Expanding the rule to cover consumer information is not necessary to carry out provisions of Title V of the Gramm-Leach-Bliley Act, plus puts the rule counter to the Act's goal of enhancing competition by providing a framework for the affiliation of banks and insurance companies.

In response to AIA's comments generally regarding the application of the proposed rule to consumer information, the Commissioner refers to her responses to comments from the Alliance. In response to AIA's first comment, that use of the word "consumer" is counter to the NAIC model and other jurisdictions, the Commissioner states that West Virginia is not required to propose an exact replica of the NAIC model and that there are in fact other jurisdictions that have proposed the rule as requiring the implementation of data safeguards for consumer, rather than customer, information.

In response to the comment from AIA that the rule as proposed exceeds the rule making authority provided by West Virginia Code Section 33-6F-1, which authorizes the Commissioner to promulgate rules necessary to carry out the provisions of Title V of the Gramm-Leach-Bliley Act, the Commissioner points out that Title V of the Act refers to both consumers and customers. Therefore, it is clear that Congress intended to require the protection of both consumer and customer information. The Commissioner disagrees that she is without statutory authority to propose a rule that requires data security standards with regard to consumer information.

2. AIA is very concerned that the rule clearly state that it does not create a private cause of action. Specifically, AIA comments:

- The Gramm-Leach-Bliley Act does not create a private right of action for violation of its standards.

- A private cause of action would create significant costs and burdens on insurance licensees that don't apply to banks that are federally regulated.

- AIA requests specific language within the proposed rule that the Gramm-Leach-Bliley Act does not contemplate the availability of private causes of action for violations of Title V standards, as well as language limiting any violation to sections 3 and 4 of the proposed rule. In addition, AIA requests language that expressly limits enforcement to the Commissioner's discretionary review under §§33-3-11 and 33-12-24.

In response to these comments, the Commissioner initially notes that due to clerical error, the proposed rule that was filed with the Secretary of State and Legislative Rule Making Review Committee on May 29, 2002, does not include West Virginia Code Section 33-12-24 within its subsection 6.1 violation provision. However, the version of the proposed rule that was posted on the Insurance Commission website includes reference to that code section within subsection 6.1. Because this was an inadvertent error that has just been discovered, the Commissioner will rewrite subsection 6.1 to read as follows:

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

In response to the comments from AIA concerning the enforcement of the rule, the Commissioner states that the rule as proposed only contemplates enforcement by the Commissioner pursuant to West Virginia Code Sections 33-3-11 and 33-12-24. The Commissioner does not believe it is necessary to clarify the enforcement provisions further. The Commissioner further declines to limit violation to sections 3 and 4 of the proposed rule because it is unnecessary. Section 5, as discussed below, contains only non-exclusive illustrations of how a licensee may implement the requirements of sections 3 and 4.

3. AIA comments that the introductory language in subsection 5.1 stating that methods other than the examples set forth in section 5 will be acceptable only if they will provide the same level of security and confidentiality of consumer information, and use of the term "shall" in subsections 5.2, 5.3, 5.4, and 5.5, have the effect of imbedding a regulatory equivalency standard within the examples, turning the examples into *de facto* standards. Specifically, AIA comments:

- AIA fears that the examples will be viewed as such by the plaintiffs' bar in future lawsuits as requirements.

- AIA suggests that section 5 be deleted entirely and that the Commissioner issue an

Informational Letter to provide examples of compliance with the rule.

In response to these comments, the Commissioner agrees that use of the word "shall" in subsections 5.2, 5.3., 5.4, and 5.5 may be confusing since the introductory language of subsection 5.1 clearly states that the section contains non-exclusive examples of how a licensee may implement the required data security standards. The Commissioner also agrees that the second sentence in the introductory language of subsection 5.1 is unnecessary, since that section provides only examples or illustrations of how to comply with sections 3 and 4. However, the Commissioner disagrees that section 5 should be deleted from the rule because the section is intended to provide illustrations that a licensee may follow for compliance. The NAIC drafted the model rule in this fashion to be specific enough to protect consumers and give licensees direction on how to comply, but still accommodate the capabilities and resources of all licensees. Based upon these responses, the Commissioner declines to delete section 5, but agrees to rewrite section 5 as follows:

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.

4. AIA opposes inclusion of subsection 5.4, which is one of the examples of how a licensee may implement the data security standards required by sections 3 and 4. Subsection 5.4 states that the licensee require its service providers to implement appropriate measures designed to meet the objectives of this rule. AIA comments that it is inappropriate to target provisions at licensees that attempt to extend regulatory authority to non-licensees. Specifically, AIA comments:

- AIA suggests deletion of subsection 5.4 entirely. In the alternative, AIA suggests retaining subdivision (a) of subsection 5.4 and deletion of subdivision (b). This would leave the service provider obligations of the licensee at "exercising appropriate due diligence in selecting its service providers," which would allow the licensee flexibility to consider data security as a factor in retaining service providers. AIA suggests that this will address any concerns about the security of customer information handled by those service providers.

In response to these comments, the Commissioner declines to delete or modify subsection 5.4. The proposed rule does not require licensees to alter their contracts with service providers. Subsection 5.4 is only an example of a method to develop and implement the requirements of sections 3 and 4 of the proposed rule. In addition, subsection 5.4 would only require that licensees check with their service providers to make sure they are meeting these requirements. The Commissioner does not believe that it is overly burdensome to expect licensees to ensure that their service providers are following the law. Licensees have reason to check to see if their service providers are meeting other contractual provisions, so it would not be difficult to do the same with this particular requirement.

Alliance
of American Insurers

June 21, 2002

Mary Jane Pickens
Associate Counsel
West Virginia Insurance Commission
P.O. Box 50540
Charleston, WV 25305-0540

RE: W.Va. Code St. R. title 114, Series 62, Standards for Safeguarding Consumer Information

Dear Ms. Pickens:

Introduction

This letter is submitted on behalf of the Alliance of American Insurers, an association of over 330 property and casualty insurers. Many Alliance members do business in West Virginia and would be subject to the proposed rule.

I appreciate you speaking with me during the week of June 3. I know your time is limited and I appreciate your directions on obtaining copies of the proposed rules.

The Alliance appreciates the Department addressing the important issue of customer information security. The Alliance also agrees strongly with basing the rule and regulation on the NAIC's Standards for Safeguarding Customer Information Model Regulation.

However, the Alliance has concerns about some aspects of the rule and regulation.

Scope

The proposed rule refers to safeguarding "consumer" information rather than "customer" information under the Gramm-Leach-Bliley (GLB) Act and the NAIC model regulation on safeguarding customer information. The proposed rule and regulation defines "consumer information" as set forth in W.Va. Code St. R. title 114, Series 57, § 2.19, that is, nonpublic personal health and financial information of not only policyholders, but third party claimants and declined applicants. Rather than narrowly limiting the scope of this new regulation to customer information, as required by the GLB Act, the Department is attempting to apply the new mandates of the regulation to a broadly defined class of "consumers," using the definition from its version of the 2000 NAIC privacy model. This extends the West Virginia rule farther than the NAIC model regulation on safeguarding customer information and farther than the safeguarding customer information provisions the GLB Act, 15 U.S.C. § 6801(b).

This creates several problems for insurers. Both Congress and the NAIC intentionally limited the scope to customers only. In the absence of specific state statutory authority, the Department can go no further. No such West Virginia statutory authority exists in this case.

3025 Highland Parkway, Suite 800 • Downers Grove, Illinois 60515
tel: 630.724.2100 • *fax:* 630.724.2190 • www.allianceai.org

To the extent that "claimants" are considered to be "consumers," Congress specifically exempted "processing insurance claims" from the disclosure portion of the GLB Act. 15 U.S.C. § 6802(e)(1)(A). Thus, Congress was well aware that claimants did not have the same status as customers/policyholders. Claims-handling practices are governed by your unfair claims practices statutes and regulations, and are not appropriate subjects for this customer information regulation.

Indeed, existing West Virginia laws create a distinction between customers (policyholders) and third party claimants. Under W.Va. Code St. R. title 114, Series 14, § 6, first party claimants, that is, policyholders, are entitled to handling of their claim within certain deadlines. However, there are no similar requirements for third party claimants, except as to notice of a statute of limitations (and first party claimants are entitled to more notice than third party claimants). The reason is because first party claimants have a contractual relationship with the insurer while third party claimants are hostile not only to the insurer, but also to the insured, the customer of the insurer. The proposed rule would create confusion by establishing two different standards for insurer treatment of third party claimants.

The distinction is important. Policyholders have an ongoing contractual relationship with the insurers, and insurers tend to have quite a bit of centrally stored information about these customers. On the other hand, claimants, particularly third-party claimants, typically have no long-term relationship with the insurer. What relationship there is may be adversarial. What little information the insurer may have is often spread out in branch offices, or held by adjusters, investigators, or attorneys. This is particularly true in cases involving independent adjusters.

In spite of how they handle "customer" as opposed to "consumer" information, Alliance members are definite about one thing: they want to be able to make the decision themselves as to the level of safeguarding applicable to "consumer," that is, claimant, information, not have it dictated by regulation. This is the approach taken by the NAIC model regulation and the GLB Act and the Alliance respectfully suggests that this is the best approach.

Title V of GLB was enacted in November of 1999. Since that time, insurers have been preparing to implement or have implemented information safeguarding practices relying upon the scope being limited to customers only. Unilaterally expanding a regulation to cover consumers as well will impose new costly and burdensome mandates and restrictions upon insurers that will ultimately translate into higher premiums for insurance consumers.

Banks and securities firms are subject only to customer information regulations already in place at the federal level. Forcing insurers to also deal with consumer information will place insurers at a competitive disadvantage.

Imposing one-state consumer information regulations will make West Virginia a less attractive market for multi-state insurers. This will translate into fewer choices for insurance consumers in West Virginia. Further, this lack of uniformity imposes additional expenses on insurers to create a special program for a single state.

Time for Compliance

The proposed rules do not provide a specific time for compliance. The NAIC model provides no guidance on this issue. Analogous federal regulations provide two years to comply as to service provider contracts in effect prior to the effective date of the regulation. *See, e.g.,* 12 C.F.R. Part 30, Appendix B, § III.G.2, giving national banks two years to comply as to service provider contracts. While the Alliance does not insist on two years to comply as to service contract

providers, the Alliance suggests six months to comply as to service providers, especially given the large size of some insurers. A longer period of time for compliance as to service contracts is needed if the rule and regulation is to apply to "consumer" as opposed to "customer" information.

The Alliance appreciates the opportunity to comment on the proposed rule and regulation. Please contact me if you have any questions concerning these comments.

Sincerely,

Patrick Watts
Assistant Vice President
Regulation, Tax, Law & Claims
Tel. 630.724.2166
pwatts@allianceai.org

G:\TAXLAW\PW\LETTERS\WV Comments Safeguarding Cust Info.doc

LAW OFFICES
SPILMAN THOMAS & BATTLE, PLLC
SINCE 1864

990 ELMER PRINCE DRIVE, SUITE 205
MORGANTOWN, WEST VIRGINIA 26505
TELEPHONE (304) 599-8175

417 GRAND PARK DRIVE, SUITE 203
PARKERSBURG, WEST VIRGINIA 26101
TELEPHONE (304) 422-6700

SPILMAN CENTER
300 KANAWHA BOULEVARD, EAST
POST OFFICE BOX 273
CHARLESTON, WEST VIRGINIA 25321-0273
TELEPHONE (304) 340-3800
FACSIMILE (304) 340-3801

333 PENCO ROAD, SUITE A
WEIRTON, WEST VIRGINIA 26062
TELEPHONE (304) 723-6980

WRITER'S DIRECT DIAL NO.

(304) 340-3829
e-mail
tcox@spilmanlaw.com

July 1, 2002

VIA HAND-DELIVERY

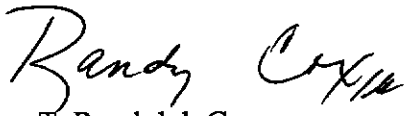
Ms. Jane Cline, Commissioner
West Virginia Division of Insurance
1124 Smith Street
Charleston, West Virginia 25301

RE: Comments – Proposed 114 CSR 62, 114 CSR 2, 114 CSR 30, and 114 CSR 20

Dear Commissioner Cline:

Enclosed are the American Insurance Association's comments to the above-referenced proposed rules.

Very truly yours,



T. Randolph Cox

TRC/lb

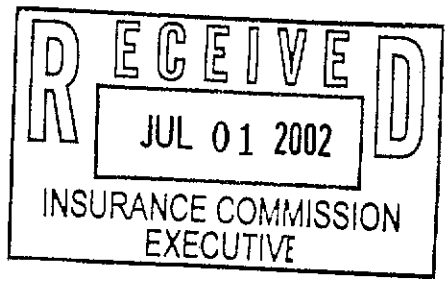
Encl.

American Insurance Association

1130 Connecticut Ave. NW
Suite 1000
Washington, DC 20036
202-828-7100
Fax 202-293-1219
www.aiadc.org

June 28, 2002

BY E-MAIL



The Honorable Jane Cline
Commissioner of Insurance
State of West Virginia
Department of Insurance
1124 Smith Street
P.O. Box 50540
Charleston, WV 25305-0540

Re: 114CSR62 West Virginia Emergency Rule – Insurance Commissioner – Series 62, Standards For Safeguarding Consumer Information

Dear Commissioner Cline:

The American Insurance Association ("AIA") has reviewed the West Virginia Department of Insurance's ("Department") emergency rule proposed to be codified at Title 114, Series 62 of the West Virginia Administrative Code ("proposed data security rule" or "proposed rule"), which seeks to implement § 501(b) of the Gramm-Leach-Bliley Act of 1999 ("GLBA"), with examples set forth in § 114-62-5 of the proposed rule. As the authority section of the proposed rule aptly notes, section 505(b)(2) of GLBA requires state insurance authorities to establish appropriate standards for financial institutions subject to their respective jurisdictions relating to administrative, technical, and physical safeguards for "customer" records and information. AIA is a trade association of major property and casualty insurance companies, representing over 410 insurers that provide all lines of property and casualty insurance throughout the United States and write more than $86 billion in annual premiums.

While we applaud the Department's decision to generally track the data security regulatory structure proposed by the Securities and Exchange Commission ("SEC") (see 65 *Fed. Reg.* 40334, 40371 (June 29, 2000), 17 C.F.R. § 248.30), rather than looking to guidelines adopted by the Federal banking agencies on February 1, 2001, 66 *Fed. Reg.* 8616, we believe that this decision has been undercut by the Department's expansion of the data security structure to include all "consumer" information. The Department's decision in this regard runs counter to the

scope of the data security model regulation recently adopted by the NAIC. It also runs counter to data security rules adopted or pending in other jurisdictions, including California, New York, South Dakota, and Utah. Each of those jurisdictions has confined its data security parameters to insurance customer information consistent with § 501 of GLBA. This section, which is quoted in the body of the proposed rule at § 114-62-1.2(a), (b), states:

> "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) Financial institutions safeguards
>
> In furtherance of the policy in subsection (a), each agency or authority described in section 6805(a) of this title shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards –
>
> (1) to insure 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**."

15 U.S.C. § 6801 (emphasis added).

As the emphasized language demonstrates, GLBA's data security standards focus on protecting customer information, **not** consumer information. This is an important distinction, since "consumers," as further defined through the NAIC model regulatory process, potentially include claimants and other individuals with whom licensees have no continuing business relationship.

The Department's proposed expansion of the data security standard to include all consumer information threatens AIA's primary goals of uniformity and operational consistency in privacy regulation across jurisdictional lines, and places West Virginia out-of-step with other insurance regulatory jurisdictions. For AIA member companies, many of which operate regionally and nationally, uniformity and consistency are necessary for three overriding reasons: (1) compliance implementation; (2) reduction in cost burden; and (3) leveling the competitive playing field. The costs of ensuring compliance increase with differing regulation. Those costs will inevitably increase where a company guesses incorrectly about a legislative or regulatory outcome and must re-tool its privacy compliance program.

In addition, an uneven insurance regulatory playing field in the area of privacy may tip the competitive balance in favor of federally regulated financial institutions (which are regulated by one standard instead of by 51 standards). If adopted as proposed, the Department's proposed data security rule would require West Virginia insurers (and other West Virginia licensees) to incur significant costs to expand their data security measures to include consumer information within the scope of their programs. These burdens will not be imposed on those financial institutions with which insurers compete, and will therefore put West Virginia licensed insurers at a disadvantage. Based on these significant impediments to the goals of uniformity and consistency, AIA must respectfully oppose the proposed data security rule as currently drafted.

Additionally, AIA is concerned that the proposed data security rule, as currently drafted, exceeds the rulemaking authority provided by W. Va. Code § 33-6F-1. That provision specifically references Title V of GLBA and requires the Department to propose rules "necessary to carry out [those] provisions...." Based on the specific parameters of § 501(b) of GLBA, it is difficult to argue that a proposed expansion of those parameters to include all consumer information is "necessary" to carry out the provisions of Title V. As a result, the proposed rule's expanded scope likely violates § 33-6F-1. Moreover, the proposed rule is not saved by § 507 of GLBA. That provision does not automatically deem that a validly-adopted state rule provides "greater privacy protection" than Title V. Such a determination must be made by the Federal Trade Commission. More importantly, where the proposed rule puts insurance companies and other insurance licensees at a competitive disadvantage, that rule conflicts with the overarching purpose of GLBA, which is "[t]o enhance competition in the financial services industry by providing a prudential framework for the affiliation of banks, securities firms, insurance companies, and other financial service providers...."

At this stage, AIA would like to respectfully note several additional concerns with the proposed data security rule that should be remedied in any subsequent draft. First, while we do not suggest that the Department has contemplated creation of private enforcement of the data security standards through the inclusion of § 114-62-6 in the proposed rule (and that section's corresponding references to W. Va. Code §§ 33-3-11 and 33-12-24), we reiterate our consistent position that any proposed data security rule should not give rise to a private right of action. This is particularly true where citations to state law are included that could be interpreted by the judiciary to create a private right of action.

We are particularly concerned with § 114-62-6 since its broad language implies that any breach of the proposed rule, including running afoul of one of the subsections denominated as "examples," will give rise to an enforceable violation. GLBA does not create any private right of action for violations of its standards. Enforcement of privacy standards under GLBA is the exclusive province of the functional financial services regulator. In addition, to the extent that the proposed

data security rule might make a private right of action available, that would generate significant costs and burdens on insurance licensees that are foreign to other federally-regulated financial institutions. In this respect, AIA suggests the addition of language to the proposed rule that specifically states that GLBA does not contemplate the availability of private causes of action for violations of Title V standards, as well as language limiting any violation to §§ 114-62-3 and 114-62-4 of the rule (the operative "regulatory" provisions). In addition, AIA recommends revising § 114-62-6 of the proposed rule to limit enforcement to the Department. The revised section, including all recommended AIA changes, would read: "Violations of **§§ 114-62-3 and 114-62-4** of this rule are subject **only** to the **Commissioner's discretionary review under** provisions of W. Va. Code §§ 33-3-11 and 33-12-24. **This section does not create or imply a private right of enforcement.**"

Second, § 114-62-5 of the proposed data security rule still contains some elements of the Federal banking guidelines as "examples," with introductory language added to clarify that the examples are illustrative, not exclusive. Our concern is compounded by the introductory language itself, which indicates that methods of implementing a data security program other than the "examples" set forth in § 114-62-5 will be acceptable only "if they will provide the same level of security and confidentiality of consumer information as the examples in this section." The use of the mandatory term "shall" in each of the examples exacerbates the problem. Such language, in each of these instances, has the effect of imbedding a regulatory equivalency standard within the examples, turning the examples themselves into de facto standards.

Even were this troubling introductory language not included in § 114-62-5, the use of any examples in the context of a rule creates the appearance of a standard for licensees to follow. In addition, rather than serving as guidance, we fear that the plaintiffs' bar will view the examples in future lawsuits as requirements. Discovery will then focus on whether a licensee adhered to an example – and, if not, why not? AIA firmly believes that the Department will avoid these problems by deleting § 114-62-5 from the proposed rule. If the Department believes that licensees require further guidance on developing and implementing an information security program, that guidance can be achieved through an informational bulletin or circular letter setting out the substance of the deleted sections, not through inclusion of examples in the proposed rule.

Third, AIA opposes inclusion of the section in the example portion of the proposed rules dealing with service provider arrangements, especially the provision mandating that licensees require service providers to implement appropriate data security protection.[1] Our concerns include: (a) the propriety and difficulty of

[1] If AIA's first or second proposed changes are adopted, the definition of "service provider" in § 114-62-2.5 will no longer be necessary. We would consider this a positive development. As currently drafted, this definition in used in the general privacy lexicon without any thought as to the consequences that come with such a broad definition. We note that the NAIC Model Privacy

provisions targeted at licensees that attempt to extend regulatory authority to non-licensees, and (b) the issuance of a requirement (see § 114-62-5.4(b)) in the guise of an example.

If the Department is not inclined to delete § 114-62-5.4 in its entirety, we recommend retention of subsection (a), and deletion of subsection (b), which directs licensees to require implementation of appropriate data security measures by its service providers and, in conjunction with a licensee's risk assessment procedures, to "take[] appropriate steps to confirm that its service providers have satisfied these obligations." By exercising "appropriate due diligence in selecting its service providers," as set forth in subsection (a), licensees will be able to determine under what circumstances service providers should be retained. Allowing the licensee flexibility to consider data security as a factor in retaining service providers will address any concerns about the security of customer information handled by those providers. Deletion of subsection (b) is also consistent with the general approach of the example section of the proposed rule (i.e., to provide general illustrative guidance, as opposed to specific data security requirements).

On behalf of AIA and its member companies, thank you for this opportunity to comment on the proposed data security rule and your consideration of the points discussed in this letter. Should the Department choose to accept AIA's recommended changes, especially the suggested refocusing of the proposed rule on customer information, we believe the Department will promulgate rules that substantially aid the security of customer information and promote compliance by all insurance licensees. If you have any questions or require further information about the concerns raised in this letter, please do not hesitate to contact me at 202-828-7175.

Respectfully submitted,

/s/

J. Stephen Zielezienski
Assistant General Counsel

cc: Taylor Cosby, AIA

Regulation does not contain a service provider definition. The Department should not use a discrete and targeted data security regulation to introduce a definitional term that may be inappropriate in a broader context. At the bare minimum, if the Department is unwilling to delete the definition, the term should be modified to limit its application to the data security context. This can be accomplished by adding the phrase "for purposes of § 114-62-5.4 of this regulation" at the beginning of § 114-62-2.5.

Insurance Commissioner
Legislative Rule
Title 114, Series 62

STANDARDS FOR SAFEGUARDING CUSTOMER 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. The rule includes, within the definition of "customer information," an application for an insurance product submitted by a consumer, regardless of whether the consumer ultimately purchases the insurance. This rule will bring the state into compliance with these directives.

Insurance Commissioner
Legislative Rule
Title 114, Series 62

STANDARDS FOR SAFEGUARDING CUSTOMER 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 Customer 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 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 customer 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. In addition to information about customers, the rule also requires applications for insurance products submitted by consumers to be subject to the data security standards. This consumer information is not included in the model rule, and may require licensees to design their standards to meet this requirement which may not exist in other states that have adopted the model rule verbatim. 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: July 26, 2002

Signature of Agency Head or Authorized Representative

JANE L. CLINE, INSURANCE COMMISSIONER

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. 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. 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 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. "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 applications for an insurance product submitted to a licensee by a consumer, 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.

STATE OF WEST VIRGINIA

Offices of the Insurance Commissioner

Legal Division

BOB WISE
Governor

JANE L. CLINE
Insurance Commissioner

July 26, 2002

HAND DELIVERED

Ms. Judy Cooper, Director
Administrative Law Division
Office of Secretary of State
State Capitol
Charleston, West Virginia 25305

Dear Ms. Cooper:

Please find herewith, one (1) copy of the following for filing:

1) Notice of Agency Approval of a Proposed Rule and Consent of Cabinet Secretary of Tax and Revenue;

2) Legislative Rule-Making Review Committee Questionnaire;

3) Brief Summary of Rule;

4) Statement of Circumstances;

5) Fiscal Note for Proposed Rule; and

6) Agency approved proposed rule entitled "Standards for Safeguarding Consumer Information" (Title 114, Series 62).

Please contact me if further information is required.

Sincerely,

Jane L. Cline
Insurance Commissioner

JLC/jz
Attachments

Post Office Box 50540
Charleston, West Virginia 25305-0540

Telephone (304) 558-0401
Facsimile (304) 558-1362