Position Statement

PRIVACY

ISSUE: DATA SECURITY

POSITION:

AIA supports state efforts to protect consumer information pursuant to Title V of the Gramm-Leach-Bliley Act of 1999 (GLBA) while preserving critical business use of such information. AIA support extends to Subsection 501(b) of GLBA, which requires functional regulators to promulgate standards to protect the security of nonpublic personal information of a financial institution’s customers.

State regulation in this area should afford an insurance licensee flexibility to develop and implement personal information safeguards that are tailored to the needs of the licensee. To this end, AIA supports the uniform adoption of data security regulations patterned after those issued by the Securities and Exchange Commission (SEC). SEC rules require financial institutions to adopt policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information. The policies and procedures must be reasonably designed to insure the security and confidentiality of customer records and information, protect against any anticipated threats or hazards to the security or integrity of customer records and information, and protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer. The SEC approach essentially codifies the requirements of § 501(b).

AIA generally supports the NAIC data security model regulation, but would propose several revisions (discussed below).
**ADVOCACY POINTS:**

- Adopting the SEC's flexible approach is supported by the manner in which Congress directed state insurance authorities to implement section 501(b). Under section 505(c) of GLBA, the federal banking agencies are to adopt the standards as guidelines, while the state insurance authorities, the SEC and the Federal Trade Commission (FTC) adopt the standards as regulations. This establishes a difference between the treatment of banking organizations and other financial institutions such as insurers. Since a violation of a rule has potentially more severe consequences than a violation of a guideline, AIA believes that this calls for additional flexibility in the manner in which the state insurance authorities implement section 501(b).

- Section 501(b) applies only to “customer” information. To the extent that states proposing expanding the data security standards to “consumer” information as well, they run the risk of imposing requirements on insurers that differ from the standards applicable to federally-regulated financial institutions. As a result, AIA opposes any expansion of the data security rules beyond customer information.

- The SEC approach is consistent with the approach followed by the two examination handbooks (market conduct and financial condition) developed by the National Association of Insurance Commissioners. Both handbooks provide specific guidance on data security parallel to the flexible approach.

- In the event that any state proposes the NAIC Data Security Model Regulation, the following modifications should be made:
  
  - *First*, the proposed regulation still contains some elements of the Federal banking guidelines as “examples,” with introductory language added to clarify that the examples are illustrative, not exclusive. The use of any examples in the context of a rule -- even where accompanied by explanatory text -- creates the appearance of a standard for licensees to follow. Those sections of the model designated as “examples” should therefore be removed.
  
  - *Second*, the proposed regulation should not include the section in the example portion of the regulation dealing with service provider arrangements, especially the provision mandating that licensees require service providers to implement appropriate data security protection. Even where retained, “examples” should not be framed as requirements. In addition, this portion of the regulation attempts to regulate non-licensees (i.e., service providers) by imposing standards on insurers.
• Third, Section 10 of the proposed regulation, which makes a violation of Sections 3, 4, or 11 an unfair method of competition or unfair or deceptive trade practice under applicable state law, needs to be deleted or revised. The NAIC needs to be mindful of the likely consequences in certain insurance regulatory jurisdictions of making a violation of the proposed data security regulation an unfair trade practice. While some state laws do not contain a private right of action for unfair methods of competition or unfair trade practices, other state laws do. In contrast, 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, making a private right of action available under the proposed regulation creates significant costs and burdens on insurance licensees that are foreign to other federally-regulated financial institutions.

BACKGROUND:

Subsection 501(b) of GLBA directs the functional financial services regulators to promulgate data security standards to protect against unauthorized access to or disclosure of nonpublic personal financial information. Based on this directive, the New York Insurance Department issued a rule that contains a general data security standard, and includes a set of non-exclusive “examples” purported to guide licensees. The New York rule has been essentially adopted by the NAIC as a model regulation.

For further information, contact AIA Associate Counsel Angela M. Gleason at (202) 828-7181, agleason@aiadc.org.

April 2012