American Insurance Association

(34)

August 25, 2000

Manager
Dissemination Branch
Information Management & Services Division
Office of Thrift Supervision
1700 G Street, N.W.
Washington, DC 20552

Re: Proposed Interagency Guidelines Establishing Standards for Safeguarding Customer Information
Docket No. 2000-51

Ladies and Gentlemen:

The American Insurance Association ("AIA") is pleased to provide its views in connection with your request for public comment on its proposed guidelines establishing standards for safeguarding customer information (the "Guidelines"). The Guidelines implement § 501 of the Gramm-Leach-Bliley Act (the "GLB Act"), which calls for the agencies to establish appropriate standards for financial institutions relating to administrative, technical and physical safeguards to protect the security and confidentiality of customer information. The AIA is the principal trade association for property and casualty insurance companies, representing more than 370 major insurance companies which provide all lines of property and casualty insurance and write more than $60 billion in annual premiums.

While insurance companies will not directly be subject to the Guidelines, the AIA believes that it is important to provide its comments to you concerning the effect the Guidelines would have on insurers. Insurers will be affected by the Guidelines as more and more companies affiliate with financial institutions subject to the jurisdiction of the federal agencies. In addition, we believe it is important for both the federal agencies and the state insurance authorities to adopt standards that are consistent and comparable, as provided in § 504(a)(2) of the GLB Act. State insurance authorities will likely consider adoption of an approach similar to that of the agencies. In view of the likely effect of the Guidelines on insurers, and in the interest of promoting that a uniform and consistent approach be taken to this matter by the functional regulators, we believe that it is appropriate for the AIA to comment on the proposed Guidelines.

1130 Connecticut Avenue, N.W., Suite 1000 ▾ Washington, DC 20036 ▾ Phone: 202/828-7100 ▾ Fax: 202/293-1219 ▾ www.aiadc.org

The AIA's comments on the Guidelines are as follows:

Section I.C.2 -- Definition of Customer Information

Section 501(a) of the GLB Act expresses Congressional policy with regard to the protection of the security and confidentiality of customers' nonpublic personal information. Section 501(b) requires the agencies to propose standards in furtherance of this policy. However, it appears that § I.C.2 of the Guidelines goes beyond the scope of Congressional policy expressed in § 501(a) by covering all records, data, files and other information of a financial institution if they contain nonpublic personal information of a customer. As a result, the Guidelines would apply to virtually all information maintained by financial institutions, not just nonpublic personal information. This would expand the scope of coverage of § 501 well beyond that intended by Congress. Accordingly, the AIA urges you for purposes of the Guidelines to define the term "customer information" as "nonpublic personal information" as defined in the rule you adopted implementing §§ 502 and 503 of the GLB Act, entitled Privacy of Consumer Financial Information (the "Privacy Rule").

Section I.C.3 -- Definition of Customer

Section I.C.3 of the Guidelines proposes to define the term "customer" in the same manner as defined in your Privacy Rule. The term "customer" does not include business customers or consumers who have not established an ongoing relationship with the financial institution. You have asked whether the term "customer" should be defined to cover these persons as well as others. The AIA believes that the Guidelines should apply only to those nonbusiness customers who have an ongoing relationship with the financial institution. Accordingly, we recommend that the term "consumer" not be expanded. We believe that the definitions applicable to section 501 of the GLBA should be consistent with the definitions used for other sections of Title V. It could prove confusing to customers and financial institutions if a different definition of the term "customer" were used in the Guidelines. If institutions choose to apply the Guidelines to nonpublic personal information they maintain about consumers or business customers, this should be a choice the institution itself should be permitted to make. Accordingly, we recommend that Guidelines retain the definition of the term "customer" as proposed.

Section II -- Standards for Safeguarding Customer Information

Section II of the Guidelines generally restates the requirements of § 501(b) of the GLB Act with regard to the elements that a financial institution's security program should encompass. Section II.B.3 provides that a financial institution's security program should protect against unauthorized access to or use of customer information, as required by § 501 of the GLB Act. However, the proposed Guidelines add the requirement that the security program also protect against unauthorized access to and use of information that could result in risk to the safety and soundness of the financial institution. The AIA believes that it is inappropriate for the agencies to expand the requirements of § 501 of the GLB Act by adding a requirement that Congress did not include. The agencies have

already addressed concerns for a financial institution's safety and soundness in § I.B, whereby you indicate that the Guidelines in no way limit the agency's authority to address unsafe or unsound practices. Because the issue of unsafe and unsound practices is already addressed elsewhere in the Guidelines, the AIA believes the Guidelines should not contain an additional requirement for which Congress has not provided. Accordingly, we recommend that the reference in § II.B.3 to safety and soundness be deleted from the Guidelines.

Section III.A.1 -- The Role of the Board of Directors

Section III.A.1 indicates the role of a financial institution's board of directors in the development and oversight of the institution's information security program. Section III.A.1.b requires the institution's board to oversee efforts to develop, implement and maintain the institution's information security program. The AIA believes that this is not the appropriate role for an institution's board of directors.

The Guidelines should not require the board to be responsible for overseeing the institution's efforts to develop, implement and maintain the institution's program. Boards of directors are typically not involved to such an extent in the institution's programs. The oversight responsibility is more properly handled by the institution's management, which is in a better position than the board to oversee the development, implementation and maintenance of the institution's programs. The role of the board should be limited to approving the policy and program that complies with the Guidelines and reviewing periodic reports by management. Accordingly, we recommend that you delete § III.A.1.b.

You ask whether the board should designate a Corporate Information Security Officer or other responsible person who would have authority to develop and administer the institution's security program. The AIA strongly opposes this requirement. The determination of whether an information officer is appropriate should be left to the institution. Accordingly, we recommend that the Guidelines permit financial institutions to choose whatever information security structure they believe is appropriate for their circumstances.

Section III.A.2 -- Management's Responsibilities

Section III.A.2 requires management to develop, implement, and maintain an effective information security program. We believe that this provision should permit a financial institution that is part of a larger organization to make use of an information security program developed by the institution's affiliate. This would enable financial institutions to harmonize their information security programs across the organization and benefit from economies of scale.

Section III.A.2.c requires management to report regularly to the Board on the status of the institution's information security program. You have asked what the appropriate reporting frequency should be. We believe it is undesirable for you to specify a reporting frequency. Because the complexity and structure of each institution's

program is of necessity unique to that institution's particular situation, we believe that the proper time interval should be left to the determination of the institution's board and management. We suggest that you amend the Guidelines accordingly.

Section III.C -- Manage and Control Risk

Section III.C.1.a provides that an institution should consider appropriate access rights to customer information. The implications of this requirement are of significant concern to the AIA. The AIA believes that it is inappropriate for the agencies to include in the Guidelines any requirement that suggests that the institution should provide customers with access rights to customer information which it maintains. This would be beyond the scope of the GLB Act and would be extremely disruptive at this time. Providing customers with access rights is a tremendously important issue for the financial services industry. The Guidelines are not the place in which this issue can or should be resolved. In the event this provision is intended to cover only employees and other service providers, we see little reason for its inclusion in the Guidelines because these parties are covered in section III.C.1.b. Accordingly, the AIA recommends that § III.C.1.a be deleted.

Section III.C.1.d provides that institutions should consider appropriate encryption of electronic customer information. The extent to which an institution utilizes encryption is one that should not be determined in the context of an information security program. This issue applies across broad areas of a financial institution's operations and should not be dealt with in a piecemeal manner by referencing the issue in the Guidelines. The AIA believes that the appropriate level and scope of encryption should be left to the determination of management, and should be done in the context of the institution's overall consideration of the extent to which encryption should be utilized by all relevant parts of the institution. Accordingly, we recommend that any reference to encryption in § II.C.1.d be deleted from the Guidelines.

Section III.C.1.f requires institutions to consider appropriate employee background checks for employees with responsibilities for or access to customer information. The issue of appropriate employee background checks, like that of encryption, should not be determined in the context of an information security program. This issue applies across all aspects of a financial institution's employment policy and should not be dealt with in the piecemeal way proposed in the Guidelines. The AIA believes that the extent to which an institution should make use of employee background checks should be left to the determination of management in the context of the institution's overall determination of its employment policy. Accordingly, the AIA recommends that the reference to employee background checks in § III.C.1.f be deleted from the Guidelines.

You also ask for comment on the degree of detail that should be included in the Guidelines regarding the risk management program. The AIA believes that the agencies should identify the various risk elements, as the proposed Guidelines do, and not specify any greater detail. Management is in the best position to determine the details of a risk

management program. Accordingly, the AIA recommends that the Guidelines not contain any greater detail regarding the elements of a financial institution's risk management program.

Section III.C.2 -- Staff Training

Section III.C.2 requires financial institutions to train staff to recognize, respond to, and report to regulatory and law enforcement agencies unauthorized or fraudulent attempts to obtain customer information. The AIA believes the Guidelines should clarify that employees should report possible violations of law to management, which then makes the appropriate reporting determination. It is entirely inappropriate for employees to make reports to regulatory and law enforcement agencies on their own. The decision to file a report concerning a possible violation of law to a regulatory or law enforcement agency is a matter that should be made by the institution's management. The rules of the agencies already require institutions subject to their respective jurisdictions to file Suspicious Activity Reports in connection with violations of law. (See 12 C.F.R. §§ 21.11; 353.3; 563.180; and 208.62.) Accordingly, the AIA suggests that the Guidelines require training of staff to report to management any unauthorized or fraudulent attempts to obtain customer information. Management would then be required by other rules to determine when and to whom to make reports.

Section III.C.3 -- Testing

Section III.C.3 requires tests of key controls, systems, and procedures to be conducted, where appropriate, by independent third parties or staff independent of those that develop and maintain the security programs. It also provides for a review of the test results by independent third parties or staff independent of those that conducted the test. The requirement to use independent third parties or staff will, of course, increase the cost of implementation and maintenance of an information security program. We believe that these additional procedures for independent testing and associated increased costs will not materially improve an institution's information security program. Testing conducted by existing employees who are accountable to management should be satisfactory. The AIA sees little reason why the Guidelines should specify that an institution should consider independent testing. In this regard, it is likely that test results will be reviewed by the institution's auditors and others. This should further reduce the need to impose additional costs on financial institutions. Accordingly, the AIA recommends that the Guidelines delete the suggestion that testing be performed and reviewed by independent third parties or independent staff.

You also ask whether the Guidelines should specify the types of security tests that should be required, such as penetration tests or intrusion detection tests. The AIA believes that the types of tests that should be conducted should be left to the determination of management.

Section III.D -- Oversee Outsourcing Arrangements

Section III.D provides that an institution must exercise appropriate due diligence in managing and monitoring its outsourcing arrangements to confirm that its service providers have implemented an effective information security program. The AIA believes that financial institutions should not be required to continually monitor the information security programs of third party service providers. This would impose an undue burden on financial institutions with very little benefit. In fact, many third party service providers are unwilling to provide specific information about their information security programs out of a concern that this could compromise the integrity and security of their operations. The AIA believes that it would prove extremely difficult for financial institutions to monitor third party service providers on an ongoing basis. A better approach would be to require financial institutions to obtain a representation or other comfort from the third party service provider to the effect that the provider's information security program is consistent with the Guidelines. Accordingly, we recommend that the Guidelines be amended to specify that financial institutions ensure that third party service providers agree to maintain information security programs that are consistent with the Guidelines.

Section III.E -- Implement the Standards

The Guidelines establish an implementation date of July 1, 2001, which is the same date financial institutions are required to comply with the Privacy Rules. In view of the extensive systems and operational changes, as well as testing requirements and consultations with service providers, that will be required to implement the Guidelines, the AIA believes that a July 1, 2001 date is very ambitious. We believe it is more realistic to establish a compliance date of December 31, 2001 for the Guidelines. This will provide financial institutions with sufficient time to develop, implement and test their privacy information systems to ensure that they comply with the Guidelines.

The AIA appreciates the opportunity to provide its comments on the proposed Guidelines. If you have any questions, please do not hesitate to call.

Sincerely,

Craig A. Berrington
Senior Vice President and
General Counsel