4/24/17, pH

(10)

AMERICAN COUNCIL OF LIFE INSURERS
FINANCIAL SECURITY FOR LIFE

Roberta B. Meyer
SENIOR COUNSEL
robbiemeyer@acli.com

August 25, 2000

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

2000 AUG 28 A 8:50

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

Ladies and Gentlemen:

These comments are submitted on behalf of the American Council of Life Insurers ("ACLI") in response to your request for public comment on your proposed guidelines implementing section 501 of the Gramm-Leach-Bliley Act ("GLBA") (the "Guidelines"). The Guidelines require the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision (the "Agencies") to establish appropriate standards for financial institutions subject to their respective jurisdictions relating to administrative, technical, and physical safeguards for customer records and information.

The ACLI is a national trade association whose 435 member companies represent approximately 73 percent of the life insurance and 87 percent of the long term care insurance in force in the United States. They also represent over 80 percent of the domestic pension business funded through life insurance companies and 71 percent of the companies that provide disability income insurance. The ACLI commends you for your effort in crafting these important Guidelines and appreciates the opportunity to submit these comments.

As insurers, ACLI member companies are not directly subject to the proposed Guidelines. However, we believe that it is important for us to comment on it for several reasons. First, to the extent that member companies affiliate or otherwise enter into business relationships with financial institutions which are subject to your agency's jurisdiction, they will be significantly affected by them. In addition, the GLBA requires the Agencies to adopt rules that are consistent and comparable. The ACLI has urged the National Association of Insurance Commissioners ("NAIC") to adopt a similar approach with regard to any model rule it may be considering for use at the state level.

1001 PENNSYLVANIA AVENUE, N.W., WASHINGTON, D.C. 20004-2599
(202) 624-2184 FACSIMILE (202) 624-2319 TDD (202) 624-2090
www.acli.com

We believe it is critically important that any rules adopted by the states be uniform from state to state and that they be consistent with, if not identical to, the standards adopted at the federal level. This is necessary in order to facilitate a smooth implementation of all the privacy provisions of the GLBA, and to avoid undermining the reasons for which the GLBA was enacted. It is our hope that the states will use the proposed Guidelines as a template in developing corresponding state rules. In order to achieve this goal, we are submitting comments on the proposed Guidelines which take into account the effect they would have if they were to be applicable to insurers.

Our specific comments are as follows:

Section I.C.2. Definition of Customer Information

Under the proposed Guidelines, the term "customer" as used in the term "customer information" does not cover 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 others. The ACLI believes that applying the Guidelines only to those who have an ongoing relationship with the institution is the appropriate approach, and we recommend that the term 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. As you are aware, under regulations adopted by the agencies earlier this year, the term "customer" was defined to include only an individual who has a continuing relationship with the financial institution. (See 65 Fed. Reg. 35162, 35166 (June 1, 2000)). The ACLI believes that it could prove confusing if a different definition of the term customer were used in the Guidelines. While many institutions may, as a practical matter, choose to apply the Guidelines to information they maintain about customers and others, this should be a choice determined by the institution itself. Accordingly, we recommend that the Agencies add to the Guidelines the definition of the term "customer" used in the Agencies' rules adopted earlier this year.

The ACLI is most concerned that the definition of "customer information" is too broad. The proposed Guidelines provide that the term "customer information" means information that contains nonpublic personal information as defined in the privacy rules adopted by the Agencies. We believe that this definition is over inclusive because it has the effect of covering a considerable portion of the records, files and information maintained by a financial institution simply because the records, files and information "contain" nonpublic personal information. We believe that this would result in a broadening of the scope of coverage of section 501 well beyond Congress's intent. Accordingly, the ACLI strongly recommends that the definition of the term "customer information" be "nonpublic personal information" as provided for in the Agencies' rules.

Section II.B.3. Standards for Safeguarding Customer Information

Section II.B.3. requires a financial institution's security program to protect against unauthorized access to and use of customer information. This requirement is contained in section 501 of the GLBA. However, the agencies have added 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 ACLI believes that it is inappropriate for the Agencies to expand the requirements of section 501 of the GLBA by adding additional requirements that Congress did not authorize. Further, the Agencies have already addressed concerns for an institution's safety and soundness in section I.B., in which you indicate that the Guidelines in no way limit your authority to address unsafe or unsound practices. Because the issue of unsafe and unsound practices is already addressed elsewhere in the Guidelines, the ACLI does not believe the Agencies should add an additional requirement to section II.B.3, particularly one that Congress has not provided for.

Section III.A.1. Involve the Board of Directors and Management

We are concerned that section III.A.1.b. the Guidelines requires a financial institution's board of directors to be involved in the process far more than is warranted.

Section III.A.1.b. requires that the institution's board oversee efforts to develop, implement, and maintain an effective information security program. The board should not be required to be involved in 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 development, implementation and oversight responsibility are functions more properly vested with an institution's management. The institution's management is in a far better position than the board to develop, implement and maintain the institution's programs.

The Agencies also ask whether financial institutions should be required to designate a Corporate Information Security Officer who would have authority to develop and administer the institution's security program. The ACLI strongly opposes this requirement. We believe that financial institutions should be free to adopt whatever information security structure they believe is appropriate to their circumstances. The determination of whether an information officer is appropriate to the circumstances should be left to the determination of the institution.

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 requirement should recognize that a financial institution is often a part of a larger organization that has established programs across its various constituent companies. Accordingly, it is important that this section be amended to provide management with flexibility to rely upon programs developed by the institution's affiliate.

Section III.A.2.c. requires that management regularly report to the Board on the status of the information security program. The Agencies have also asked the appropriate frequency of management reports to the board of directors. We believe it is undesirable for the Agencies to specify a particular time interval for this reporting. Because the complexity and structure of each institution's program will be 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 the Guidelines be amended accordingly.

Section III.C.1. Manage and Control Risk

Section III.C.1.a. requires the institution to consider appropriate access rights to customer information. The implications of this requirement are of significant concern to the ACLI. Although as a matter of policy we generally support providing customers with access to customer information, we strongly oppose to inclusion in the Guidelines of any requirement that suggests that the institution should provide customers with access rights to customer information. This would be beyond the scope of the GLBA. Providing customers with access rights is an extremely important issue for the financial services industry that cannot and should not be addressed indirectly through the Guidelines. In this regard, if the provision is intended to cover only employees and other service providers, there is no need for the provision because these parties are covered in section III.C.1.b. Accordingly, the ACLI urges that section III.C.1.a be deleted.

Section III.C.1.d. requires institutions to consider appropriate encryption of electronic customer information. The issue of encryption is one that applies across broad areas of a financial institution's electronic data processing operations. The ACLI believes that it should not be addressed piecemeal in the Guidelines. Rather, the appropriate level and scope of encryption should be left to the determination of management in the context of the institution's overall consideration of what level and type of encryption is appropriate for the institution as a whole. Accordingly, we recommend that any reference to encryption be deleted from the Guidelines.

Section III.C.1.f. requires institutions to consider appropriate dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information. We are concerned that this requirement could prove extremely burdensome. For example, conducting background checks on employees would prove very costly and may not produce information that would prove to be of value to the institution. In an insurance company, like most banks, almost *all* employees have responsibilities for or access to customer information. Therefore the issue of whether or not to conduct employee background checks is an issue that is more properly addressed as part of the institution's overall employment policy rather than on an *ad hoc* basis as part of the Guidelines. Therefore, we suggest that the words "employee background checks" be deleted.

Section III.C.2. Staff Training

Section III.C.2. requires training of staff to recognize, respond to, and report to regulatory and law enforcement agencies any unauthorized or fraudulent attempts to obtain customer information. We are concerned about staff making 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 is properly within the domain of management of the institution. Individual employees should not be required to make such reports. In any event, the rules of the Agencies already require the filing of Suspicious Activity Reports for violations of law. (See 12 C.F.R. §§ 21.11; 353.3; 563.180; and 208.62.) In view of this requirement, the ACLI believes that there is little reason to incorporate such a reporting requirement in the Guidelines for violations of law. Accordingly, we suggest amending this section to require training of staff to report unauthorized or fraudulent attempts to obtain customer information to management. This will ensure that potential violations receive appropriate attention from management. Management would then be required by other agency rules to determine whether to make reports to regulatory and law enforcement authorities. We also suggest an amendment to require training "as appropriate" in order to ensure that the rule gives necessary flexibility in the design and implementation of staff training programs.

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, and that there be 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 necessity increase the number of people that will have access to customer information and will cause persons who otherwise might not see customer information to see it. Moreover, we believe these requirements are overly restrictive and will add undue complexity and costs to the testing process. The ACLI believes that this requirement is inappropriate and would impose an undue cost on financial institutions without significant additional benefit. Testing conducted by existing employees who are accountable to management should be satisfactory. The test results will undoubtedly be reviewed by the institution's auditors, alleviating the need to impose these additional costs on financial institutions. Accordingly, we urge deletion of the last two sentences of this section which require that testing be performed and reviewed by independent third parties or independent staff.

The Agencies also asked whether the Guidelines should specify the types of testing that should be conducted. The ACLI 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. requires that the "bank 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 . . ." We are concerned that the requirement of monitoring outsourcing arrangements may be construed to require overly burdensome internal audits and policing of every third party with which a bank has outsourcing relationships. We urge deletion of this requirement.

We appreciate the Agencies' consideration of our concerns in relation to the proposed Guidelines and would be pleased to answer any questions relating to the above.

Sincerely,

Roberta B. Meyer