

900 Nineteenth St. NW, Ste. 400
Washington, DC 20006

TEL: (202) 857-3100

FAX: (202) 296-8716

E-MAIL: info@acbankers.org

http://www.acbankers.org

11



August 25, 2000

Communications Division
Office of the Comptroller of the Currency
250 E Street, S.W., Third Floor
Washington, DC 20219
[Docket No. 00-13]

Ms. Jennifer J. Johnson, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, N.W.
Washington, DC 20551
[Docket No. R-1073]

Mr. Robert E. Feldman, Executive Secretary
Attn: Comments/OES
Federal Deposit Insurance Corporation
550 17th Street, N.W.
Washington, DC 20429
[RIN 3064-AC39]

Manager, Dissemination Branch
Office of Thrift Supervision, Information Management & Services Division
1700 G Street, N.W.
Washington, DC 20552
[Docket No. 2000-51]

Re: Interagency Guidelines Establishing Standards for Safeguarding Customer Information
and Recession of Year 2000 Standards for Safety and Soundness
65 Fed. Reg. 39472 (June 26, 2000)

Dear Sir or Madam:

America's Community Bankers (ACB) is pleased to comment on the proposed interagency guidelines¹ for establishing standards for safeguarding customer information promulgated pursuant to Title V, Section 501(b) of the Gramm-Leach-Bliley Act of 1999 (GLBA)². The GLBA requires each of the federal banking regulatory agencies (agencies) to establish appropriate standards for financial institutions to protect confidential customer information³. America's Community Bankers represents the nation's community banks of all charter types and sizes. ACB members pursue

¹ 65 Fed. Reg. 39472 (June 26, 2000).

² Pub. L. No. 106-102 (Nov. 12, 1999).

³ Pub. L. No. 106-102, Title V, Section 501(b) (Nov. 12, 1999).

1000 AUG 28 A 8:50
DISSEMINATION DIVISION

progressive, entrepreneurial and service-oriented strategies in providing financial services to benefit their customers and communities.

ACB generally supports the proposed guidelines. We believe that these standards must be in a form that provides as much flexibility as possible for insured institutions, their customers, and the entities with whom they do business or have third party arrangements. We make specific comments and suggestions in response to questions raised in the proposal.

Summary of Proposal

Under the proposal, each financial institution would be required to create, implement, and maintain a comprehensive information security program appropriate to the size and complexity of the institution, and the nature and scope of its activities. Each institution would be required to create a written plan to manage and control potential risks to the security and confidentiality of customer information. This plan must be tested and adjusted on a continuing basis to account for changes in technology and any internal or external threats to information security. Additionally, each institution's program must be overseen by its board of directors, assisted by regular reports from management about the status of the program.

The statute requires that the standards be implemented in the same manner, to the extent practicable, as standards prescribed by section 39(a)⁴ of the Federal Deposit Insurance Act. Section 39(a) authorizes the agencies to establish operational and managerial standards for internal controls, information systems, and internal audits. The agencies have promulgated guidelines to implement these standards. Section 39(a) previously was used to implement Y2K safety and soundness standards for insured depository institutions.

General

ACB generally supports the creation of standards for safeguarding the security and confidentiality of consumer information and urges the agencies to issue these standards in the form of guidelines rather than regulations. These guidelines should emphasize the parameters of an effective information security program, while allowing an institution the flexibility to exercise discretion in adopting a program that best fits its business and operations based on its size and the complexity of its information sharing arrangements. Appropriate and flexible guidelines will help provide community banks with a benchmark to measure and assess their information security practices. Overly detailed and rigid guidelines, however, risk creating costly compliance requirements for insured institutions that are not placed on less-regulated competitors offering financial and related services.

⁴ 12 U.S.C. 1831s.

The proposed guidelines are vague in terms of indicating the scope of the required standards and what actions would constitute compliance. In the rule of construction as part of, the final rule for "Privacy of Consumer Financial Information"⁵ the agencies provided examples and sample clauses that, if followed or used, constitute compliance with the rule. Similarly, the final guidelines should provide, wherever possible, examples or sample benchmarks that, if followed or met, also would constitute compliance. While the guidelines should in and of themselves be as flexible as possible, the goals of the standards should be firmly and clearly stated when they are issued in final form.

Examples are important, and should be used wherever possible, but any guidelines must properly recognize that each community bank is unique, as are its information sharing arrangements. Therefore, examples should be used to provide banks with guidance, rather than a strictly required process for compliance. ACB also agrees that guidelines for information security programs must be appropriate to the size and complexity of the scope of information sharing arrangements. However, ACB strongly urges that any such guidelines be focused on the complexity and breadth of information sharing arrangements, and not solely on the size of an institution. Within ACB's membership, there are large community banks with relatively modest information sharing arrangements and smaller institutions that use third party partnerships to conduct activities that a larger institution may conduct in-house.

ACB members have an outstanding record of protecting the confidentiality and security of consumer information. Customer trust is one of the cornerstones of the business relationships that exist for community banks. These institutions compete with non-banks offering similar products in today's fast moving and increasingly competitive financial marketplace; the trust they have earned provides them with a key competitive edge. For this reason, community banks have protected and will continue to protect the confidentiality of consumer information as part of their business practices, while they look for and engage in information sharing arrangements that offer tremendous benefits for their customers, their communities and consumers.

Specific Questions

In the preamble, the agencies ask several questions. ACB has identified the following questions as posing special concerns for community banks of all charter types and sizes:

1. Should the final standards be issued in the form of guidelines or regulations?

ACB strongly believes that the standards for safeguarding consumer information should be issued in the form of guidelines rather than regulations. By establishing the standards in the form of guidelines, the agencies preserve the ability to respond quickly by adapting the guidelines to emerging developments. Furthermore, ACB believes it was the intent of Congress to have these standards issued in the form of guidelines, as illustrated by the fact

⁵ 65 Fed. Reg. 35162 (June 1, 2000).

that Congress established specific rulemaking requirements for other privacy related elements of Title V of the GLBA⁶.

The agencies, however, should refrain from continuously revising the standards once they have been adopted in final form. In promulgating the final guidelines, the agencies should establish the scope of the guidelines. The guidelines should be structured such that institutions will be able to develop the strategies they need to comply with the final standards. Community banks, in particular, will need to be able to identify the minimum level of compliance as well as some guidance as to the maximum limits for which the agencies will look. Without such general parameters, community banks will be not be able to accurately determine the procedures they need to follow to meet the requirements of the guidelines. Another detrimental effect may be that community banks will be less willing to engage in activities or information sharing arrangements that better serve their customers if the guidelines reflect standards that require significant compliance resources without any guidance as to the parameters of required activity.

2. *What impact would this proposal have on community banks?*

Community banks represent a wide range of financial institutions with varying information sharing arrangements. Many of these institutions have limited resources to dedicate towards continuously maintaining information security programs, establishing dual-control procedures, and overseeing outsourcing arrangements. In some community banks, a single individual may be responsible for information security, in addition to other critical safety-and-soundness related activities. In order to minimize the burden to community banks, the proposed guidelines should allow an institution maximum flexibility in developing a risk management program that is appropriate to the sensitivity and complexity of its information handling procedures. For example, smaller institutions often rely more on outsourcing arrangements than do their larger competitors because they do not have the resources in-house or such arrangements are more appropriate to their needs. Therefore, they do not have the same resources to establish elaborate information security programs. Because the guidelines already require monitoring of outsourcing arrangements, the agencies should take this into account with regard to internal in-house information protection requirements.

ACB suggests that the agencies include in the final guidelines a check list that can be given to vendors to identify minimum standards. Such a list would be especially useful for community banks that do not have many third-party arrangements and also do not have the resources to devote to monitoring contractual arrangements. An example of the type of list is one of the checklists the agencies developed for purposes of determining compliance with Y2K preparedness guidelines for institutions and their vendors.

3. *Are the standards reasonable and realistic for community banks?*

⁶ Pub. L. No. 106-102, Title V, Section 504(a) (Nov. 12, 1999).

⁷ Pub. L. No. 106-102, Title V, Section 504(a) (Nov. 12, 1999).

ACB commends the agencies for establishing a flexible standard for information security programs that is “commensurate with the sensitivity of the information as well as the complexity and scope of the bank⁸.” However, the proposed standards for developing a risk management plan may be overly comprehensive for some community banks. Specifically, ACB believes that the requirement under Part III.C that each bank “shall” develop a comprehensive risk management plan that consists of fifteen different items ranging from basic staff training to consideration of third party internal control testing is overly exhaustive⁹.

ACB suggests that less specific standards are needed to ensure that community banks are able to protect consumer information while preserving their ability to effectively manage their institutions. We suggest that the agencies establish a less detailed but not necessarily less rigorous standard for non-complex institutions. Again, the determination of whether an institution is non-complex is based on business strategy and not size. For example, the agencies could provide for less specific standards for non-complex institutions by substituting the word “shall” in Part III.C with a more flexible standard such as “should consider...” while maintaining the original language for other institutions. The agencies each have implemented risk focused examination procedures, and we suggest that if an institution is found to require more specific direction, the agencies have the supervisory tools to impose additional requirements.

4. *Should the scope of the guidelines apply to records regarding all consumers, the institution's consumer and business clients, or all of an institution's records?*

ACB strongly urges the agencies not to expand the definition of “customer” beyond the definition found in the final rule for “Privacy of Consumer Financial Information”.¹⁰ We do not believe that the scope of the proposed guidelines should apply to all records of the institution. It is important that the definitions of terms like “customer” used in the final privacy regulation and final guidelines be consistent. Further, as suggested by the agencies, it is likely that some institutions will establish systems that take all of the records into account, but we strongly oppose the the inclusion of an expanded definition as part of the guidelines and the added compliance burden it would necessarily impose. In addition, Section 501(b) of the GLBA specifically uses the term “customer” in referring to these guidelines.¹¹

5. *How frequently should reports be made to the institution's Board of Directors regarding the institution's information security program?*

Each institution should be allowed to adopt reporting guidelines for involving the board of directors and management that best fits its organization and management philosophy. While reporting intervals will vary depending on the composition of the institution's operations and

⁸ 65 Fed. Reg. 39488, Part II.A (June 26, 2000).

⁹ 65 Fed. Reg. 39488, Part III.C (June 26, 2000).

¹⁰ 65 Fed. Reg. 35162 (June 1, 2000).

¹¹ Pub. L. No. 106-102, Title V, Section 501(b) (Nov. 12, 1999).

information handling practices, board directors and senior management of institutions recognize their responsibility to ensure that confidential information is protected. For some institutions, a quarterly review of its information security plan may be appropriate and desired. Other institutions may find that an annual review may be the most efficient and practical use of executive resources. ACB advises that the guidelines should not specify a recommended reporting interval, only one that is appropriate to the institution. We suggest that the guidelines require that an institution's board of directors review the policy at least annually or more frequently if changes are made to the plan. This is the standard for review for other policies required to be adopted by the board.

6. *Should each institution be required to designate a specific individual responsible for administering its information security program?*

ACB recommends that the guidelines should not specify that a specific individual be responsible for administering its information security program. As previously discussed, staff within community banks are often responsible for a variety of duties. Many community banks may choose to designate a single individual to be responsible for developing and maintaining an institution's information security program; however, it should be the goal of the standards wherever possible to allow institutions to use their discretion for determining how best to effectively administer their information security program.

7. *Should specific types of security tests, such as penetration intrusion detections tests, be required?*

The proposed standards require that each institution's risk management plan establish policies and procedures that consider various information security precautions. With the rapidly changing nature of technology, standards that require specific types of tests could become obsolete and ineffective in short time. ACB recommends that the information security program requirement focus on identifying the goals of security testing and allow institutions to develop whatever types of security testing approach they determine appropriate. If the institution has retained a consultant in this area, that organization or person should be allowed to make the determination.

8. *Should the tests be conducted by persons who are non-employees of the institution?*

Part III. C.3 of the proposed guidelines requires that each institution shall conduct testing of their information security program "where appropriate" by independent third parties or independent staff; and that the results of this testing shall be reviewed by independent third parties or independent staff not involved in conducting the evaluation. ACB views this requirement for security testing as potentially burdensome depending on the complexity of the institution. While we support the inclusion of standards that will assist community banks in operating safely and soundly, we believe that they should have as much flexibility as possible in determining the level of information security program testing required. Again, the complexity of each institution's information sharing arrangements should be a guide to how stringent the testing must be. Further, the expertise of the management and other staff performing the information sharing tasks should be taken into account. At a minimum, for

those institutions that are non-complex, we suggest that third party testing be required only periodically and that the institution must demonstrate to its examiners that management and other staff understand the importance of maintaining the integrity of the information and the process developed.

9. *How should the guidelines address the appropriate treatment and oversight of outsourcing arrangements?*

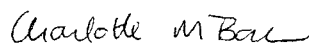
Many community banks outsource information- and data-related activities. In order to protect themselves from liability, banks generally include clauses requiring confidentiality of the information provided to outside service providers. While community banks are willing to work hand-in-hand with their outside service providers in meeting the required standards, they should not be required to police the activities of those service providers. Nor should they be held liable to other parties if there is a breach on the part of the outside service provider, if a confidentiality clause has been included in the contract. Just as the final rule for "Privacy of Consumer Financial Information" does not require financial institutions to police the activities of third parties receiving nonpublic personal information from them, so too should the final guidelines not impose a policing role to banks vis a vis outside service providers. An active policing requirement will limit or may even eliminate activities in which community banks will be able to engage.

It is important for community banks and third parties with whom they do business to have a cooperative relationship in serving the needs of their customers. Community banks must take the responsibility to do the necessary due diligence prior to entering contracts with third parties, but the third parties must live up to their obligations. Contracts must be drafted in such a way as to allocate the liability appropriately. Again, the lessons of Y2K can be applied in this area. We suggest that the standards included in the guidance issued by the agencies for purposes of Y2K compliance should be applied here.

Conclusion

ACB appreciates the opportunity to comment on this important matter and supports the agencies in their efforts to draft effective standards for safeguarding customer information. We stand ready to work with the agencies to implement the final guidelines. If you have any questions, please contact the undersigned at (202) 857-3121 or Rob Drozdowski at (202) 857-3148.

Sincerely,



Charlotte M. Bahin
Director of Regulatory Affairs and
Senior Regulatory Counsel