

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



October 10, 2000

Secretary  
Federal Trade Commission  
Room H-159  
600 Pennsylvania Avenue, NW  
Washington, DC 20580

Re: Gramm-Leach-Bliley Act Privacy Safeguards Rule  
16 CFR Part 313 - Comment  
Privacy of Customer Financial Information—Security  
65 Fed. Reg. 54186 (September 7, 2000)

Dear Sir or Madam:

America's Community Bankers is pleased to comment on the advance notice of proposed rulemaking<sup>1</sup> (ANPR) issued by the Federal Trade Commission (FTC) seeking input on establishing standards for safeguarding customer information pursuant to Title V, Section 501(b) of the Gramm-Leach-Bliley Act of 1999 (GLBA).<sup>2</sup> ACB represents the nation's community banks of all charter types and sizes. ACB members pursue progressive, entrepreneurial and service-oriented strategies in providing financial services to benefit their customers and communities.

ACB believes that the standards developed to implement Section 501(b) of the GLBA must be in a form that provides as much flexibility as possible for financial institutions, their customers, and the entities with whom they do business or have third party arrangements. We request that when the FTC issues its proposal and takes final action that it be in the form of guidelines such as those proposed by the federal banking agencies. We make specific comments and suggestions in response to questions raised in the ANPR.

### **Summary of Proposal**

The GLBA requires that the FTC, federal banking agencies, and the Securities and Exchange Commission (SEC) establish appropriate standards to protect confidential customer information.<sup>3</sup> The federal banking agencies issued proposed guidelines on an interagency basis on June 26, 2000.<sup>4</sup> The SEC incorporated the required standards into its final rule on the privacy of customer information. The FTC however has determined that it needs additional

<sup>1</sup> 65 Fed. Reg. 54186 (September 7, 2000)

<sup>2</sup> Pub. L. No. 106-102 (November 12, 1999).

<sup>3</sup> Pub. L. No. 106-102, Title V, Section 501(b) (November 12, 1999).

<sup>4</sup> 65 Fed. Reg. 39471 (June 26, 2000).

information on how to achieve the goals of Section 501(b) of the GLBA for the diverse range of financial institutions subject to the FTC's jurisdiction. The ANPR seeks public comment on a range of questions concerning the scope and potential requirements of any guidance or regulation that will be proposed for establishing standards for safeguarding customer information.

## **General**

ACB generally supports the creation of standards for safeguarding the security and confidentiality of customer records and information. These standards should be appropriate and flexible, and provide financial institutions with a benchmark to measure and assess their information security practices. Overly detailed and rigid requirements, however, risk creating costly compliance requirements for financial institutions that are not placed on other industries.

Any guidelines or regulations issued by the FTC should establish the scope of the required standards and what actions would constitute compliance. In the rule of construction found in the final rule for "Privacy of Consumer Financial Information",<sup>5</sup> the FTC provided examples and sample clauses that, if followed or used, constitute compliance. Similarly, any guidelines or regulation should provide, wherever possible, examples or sample benchmarks that, if followed or met, also would constitute compliance. While the standards 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 financial institution is unique, as are its information sharing arrangements. Therefore, examples should be used to provide financial institutions 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 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 institutions with relatively modest information sharing arrangements and smaller ones 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 our member institutions. 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, our member institutions have protected and will continue to protect the confidentiality of consumer information as part of their business practices, while they

---

<sup>5</sup> 65 Fed. Reg. 33646 (May 24, 2000).

look for and engage in information sharing arrangements that offer tremendous benefits for their customers, their communities and consumers.

### **Specific Areas for Comment**

In the ANPR, the FTC asks questions about specific aspects of the information security. ACB has identified the following areas as posing special concerns for our members:

#### *1. Range of Information Subject to Any Guidelines or Regulation*

ACB strongly urges the FTC not to expand the scope of any guidelines or regulation beyond the statutory designation of “customer records and information.” When it passed the GLBA, Congress made a specific distinction between the “customers” and “consumers” of a financial institution and how they are to be treated under Title V of the GLBA. For example, Title V requires a financial institution to provide a privacy notice to each of its “customers” no less than annually; whereas a “consumer” is entitled to an initial privacy notice only if the financial institution is going to disclose his or her nonpublic personal information to a nonaffiliated third party. Given that Section 501 of the GLBA explicitly states that its requirements apply to “customer records and information,” any guidelines or regulation should not be extended to cover information provided by other individuals, including “consumers” who are not “customers” of the financial institution. If a financial institution determines that it is necessary or more feasible to apply the established standards to other records and information, it should be allowed to make that determination on its own. “Customer records and information” should therefore be limited to the nonpublic personal information, as defined in the final rule on the privacy of customer information, of customers.

#### *2. Small Financial Institutions*

ACB commends the FTC for recognizing the importance of not unduly burdening the ability of small financial institutions to serve consumers. Small financial institutions generally have more limited resources to dedicate towards continuously maintaining information security programs, establishing dual-control procedures, and overseeing outsourcing arrangements. For example, in some financial institutions, 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 small financial institutions, any guidance or regulation 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.

In its comment letter of August 25, 2000 to the federal banking agencies, ACB commended 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 bank.”<sup>6</sup> However, the proposed standards issued by the federal banking agencies for developing a risk management plan may be overly comprehensive for some community

---

<sup>6</sup> 65 Fed. Reg. 39488, Part II.A (June 26, 2000).

banks. Specifically, ACB believes that the requirement under Part III.C that each financial institution “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 exhaustive.<sup>7</sup> ACB suggests that the FTC avoid establishing such overly comprehensive standards in any guidance or regulation that it develops.

### 3. *Specificity of any Guidance or Regulation*

ACB suggests that overly specific standards are not needed to ensure that financial institutions are able to protect consumer information. We suggest that the FTC consider a less detailed, but not necessarily less rigorous standard for non-complex institutions than was proposed by the federal banking agencies. Again, the determination of whether an institution is non-complex should be based on business strategy and not size. For example, the FTC could provide for less specific standard for non-complex institutions by substituting the word “shall” in Part III.C of the banking agencies proposal with a more flexible standard such as “should consider...” while maintaining the original language for other institutions. This approach is consistent with the federal banking agencies risk focused examination procedures.

### 4. *Statutory Objectives*

ACB urges the FTC to develop a proposed rule that establishes the parameters of effective standards for administrative, technical, and physical safeguards, 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. Therefore, we strongly discourage the FTC from including in any guidance or regulation it proposes overly specific or burdensome requirements on financial institutions.

For example, any proposed guidance or regulation should not require specific minimum steps that a financial institution must take to provide for the physical security of its customer records and information. At the same time, however, the inclusion of a list of possible measures that a financial institution could take in this regard – such as shredding discarded paper records -- would be useful to help meet the goals of any guidance or regulation.

Similarly, we would discourage any requirement that a financial institution designate a specific employee to be responsible for monitoring internal access to customer records and information. 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 carry out the goals of any guidelines or regulation that are proposed.

---

<sup>7</sup> 65 Fed. Reg. 39488, Part III.C (June 26, 2000).

ACB also discourages the imposition of any requirement specifying the types of security tests that might be used to carry out the goals of any guidance or regulation. 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.

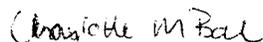
*5. Consideration of Other Agencies' Proposed Guidelines*

ACB generally believes that, wherever possible, any guidance or regulation issued to implement Title V of the GLBA should be uniform. This is crucial to preserve the competitive equity between regulated insured financial institutions and their non-insured financial services competitors. The marketplace should allow insured depository institutions and non-insured financial services organizations to compete based on price and quality of services. The FTC should avoid creating any guidance or regulation that differs significantly in scope and requirements from that of the proposed guidelines issued by the federal banking regulators.<sup>8</sup> Furthermore, ACB suggests that the FTC consider delaying issuing any proposed guidance or regulation until the federal banking regulators' corresponding final guidance is issued.

**Conclusion**

ACB appreciates the opportunity to comment on this important matter and supports the FTC in their efforts to draft effective standards for safeguarding customer information. We stand ready to work with the FTC as it develops its guidelines or regulation. 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

---

<sup>8</sup> 65 Fed. Reg. 39471 (June 26, 2000)