48,415 (9)

2000 AUG 24 P 4:09

JOHN J. BYRNE
SENIOR COUNSEL &
COMPLIANCE MANAGER
REGULATORY & TRUST AFFAIRS

1120 Connecticut Avenue, N.W.
Washington, D.C. 20036
(202) 663-5029
FAX: (202) 828-5052
INTERNET: jbyrne@aba.com

August 23, 2000

Ms. Jennifer J. Johnson
Secretary
Board of Governors of
the Federal Reserve System
20th and C Streets, NW
Washington, D.C. 20551
Attention: Docket No. R-1073

Mr. Robert E. Feldman
Executive Secretary
Comments/OES
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, D.C. 20429
Attention: Comments/OES

Communications Division
Office of the Comptroller of the Currency
250 E Street, SW
Washington, D.C. 20219
Attention: Docket No. 00-13

Manager, Dissemination Branch
Information Management & Services Division
Office of Thrift Supervision
1700 G Street, NW
Washington, DC 20552
Attention: Docket No. 2000-15

Dear Sir/Madam:

The American Bankers Association ("ABA") is pleased to take this opportunity to comment on the joint notice of proposed rulemaking on proposed Guidelines establishing standards for safeguarding customer information published to implement sections 501 and 505(b) of the Gramm-Leach-Bliley Act (Pub. L. 106-102) ("GLB"), signed into law on November 12, 1999. Section 501 requires the banking agencies to establish "appropriate" standards relating to administrative, technical, and physical safeguards for customer records and information.

ABA brings together all elements of the banking community to best represent the interests of this rapidly changing industry. Its membership – which includes community, regional and money center banks and holding companies, as well as savings associations, trust companies and savings banks – makes ABA the largest bank trade association in the country.

The banking industry has a long history of having the strongest protections against unauthorized access to customer information. A 1997 report of the President's Commission on Critical Infrastructure Protection ("Critical Foundations: Protecting America's Infrastructure") concluded that the "modern US financial system never has suffered a debilitating catastrophe, and for that reason among others carries an extraordinarily high level of global confidence." In addition, the financial

services industry announced a set of privacy principles in 1997 that emphasizes the need for financial institutions to "maintain appropriate security standards and procedures regarding unauthorized access to customer information."[1] It is clear that all institutions already have policies and procedures regarding the protection of customer information. Therefore, ABA believes that the agencies should continue to develop guidelines that provide a degree of flexibility rather than the rigidity of a regulation to address this important area.

*The following are responses to the various sections of the proposal as well as to the specific questions posed by the agencies.*

1. **Should these Standards be Regulations or Guidelines?**

Section 501 of title V of Gramm-Leach-Bliley does not mandate that the standards for protection of nonpublic personal information be issued as regulations. Financial institutions already receive a plethora of guidance concerning information technology procedures and are already examined in this area. [2] In addition, financial institutions already possess security policies and procedures that are developed on a bank-by-bank basis, factoring in the size and structure of each institution. We believe that the goal of having effective policies in security and confidentiality of customer information is already being met by the industry. It should also be noted that the issuance of regulations would simply open up the potential for technical violations, and guidelines have been proven to work effectively. For example, the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA) mandated that the banking agencies prescribe standards for safety and soundness. The agencies responded by creating interagency guidelines. The agencies also issued interagency guidelines for real estate lending. [3] Therefore, ABA urges the agencies to consider several modifications to this proposal and issue the final product as agency guidelines.

2. **Impact of the Proposed Guidelines on Community Banks.**

The agencies seek comment on the impact of this proposal on community banks. Given the fact that community banks do operate with limited resources and personnel, it remains imperative that any final

---

[1] The ABA Task Force on Responsible Use of Customer Information developed voluntary guidelines in that were released on June 6, 2000. Among other things, these guidelines reaffirmed the industry commitment to maintaining confidentiality and security if customer data.

[2] See, for example, OCC release NR-98-13 (February4, 1998) where the Comptroller of the Currency emphasizes the importance of technology risk assessment. In December 1997, the FDIC issued "Security Risks Associated with the Internet", a paper from which much of this notice of proposed rulemaking uses as a guide.

[3] See, Part 12 CFR 364.101 and 365.

guidelines allow community banks the flexibility to continue using their existing information security programs in their current format. According to one of our members, "Requiring community banks to develop a 'duplicate' program just for the purpose of complying with this program would be a poor use of our time and resources."

3. **Definitions.**

ABA strongly urges the banking agencies not to go beyond the scope of these proposed guidelines and cover records of the institution's business clients. Section 501 of Gramm-Leach-Bliley refers to "customer" information, which the agencies have interpreted as not including business customers. Of course, section 509 (Definitions) makes clear that the information covered under the new law (and subsequent regulations) covers information provided by consumers not businesses. There is no policy reason to expand the definition for purposes of an institution's security program and such change may prove costly to all institutions.

4. **Rescission of Y2K Standards for Safety and Soundness**

We agree with the decision to rescind the Year 2000 Safety and Soundness Guidelines for obvious reasons. ABA would like to mention, however, that the agencies deserve tremendous credit for working with the industry to address jointly the major challenges that Y2K presented all of us. The series of guidances issued by the agencies were extremely helpful and served to remind many in the industry to devote the necessary resources to the effort to protect the institution and to maintain the trust of our customers. We urge the agencies to follow the Y2K 'template' and to continue to provide guidances to the industry on all aspects of security and confidentiality.

5. **Objectives for the Institution's Information Security Program**

The agencies have requested comment on whether there should be are alternative approaches for developing an information security program to those listed in Section II of the proposal. Section 501 of GLB requires the agencies to "establish appropriate standards" for customer information security. The law also requires that the safeguards protect against unauthorized access to or use of customer information that would result in "substantial harm or inconvenience" to any customer. Therefore, there is no need to include any reference to "inconvenience" as a standard for appropriate customer information protection in the proposed guidelines. The industry has long believed in the need to limit employee access to information and the convenience of the customer, while important in the general sense, should not adversely affect the priority of having a strong information security program. Moreover, if customers feel they are inconvenienced they will move to another institution.

6. **Involvement of the Board of Directors**

The proposal outlines the responsibilities of directors and management of financial institutions in overseeing the customer information protection program. For example, the proposal anticipates having the Board approve the institution's security policy and to oversee efforts to "develop, implement, and maintain an effective information security program, including the regular review of management reports."

ABA agrees with the need to have security programs supervised at high levels of the institution but suggests that the goal of institution-wide support of the program can be achieved by permitting the board to delegate authority to senior management for approval and oversight of the security program. The overall degree of board involvement in the specifics of the security program should be at the discretion of the institution. This would allow institutions to base their determination of board involvement on the complexity of the program as well as the overall organizational structure.

The agencies also seek comment on the appropriate frequency of reports to the board. Reporting to the board any activity, by its very nature, demands flexibility. For example, the requirement that financial institutions file reports on the number and content of "Suspicious Activity Reports" or SARs[4] allows banks to notify their boards of directors or subcommittees of the board. This 'flexibility' should be permitted to the institution for the filing of information security reports. The SAR regulations also allow the institution to report the SARs at regular intervals rather than immediately following the filing of the SAR, unless the filing is for a serious crime. Similarly, all institutions should have the option of deciding the frequency of the filing of reporting to the board. For example, material information should be reported more frequently that routine information.

Another ABA member pointed out that "Due to the limited resources of community banks, it would be beneficial if the reporting could be limited to an annual report to the Board and more frequent reports would only be required if there were any attempted or actual security breaches or violations."

7. **Factors for Risk Assessment and Risk Management**

The proposed guidelines also list a number of factors that an institution "should" consider in evaluating program adequacy. While we recognize that this proposal is drafted as guidance to the industry, we urge the agencies to clarify that the factors are simply suggestions and are in no way mandatory to compliance with information security standards. The final guidelines should state that institutions have the option of performing a security self-assessment by utilizing these factors "or any other that the institution deems appropriate."

---

[4] See 12 CFR 208 for the Federal Reserve Board's regulation on SARs. All of the other banking agencies have similar regulations.

It is unclear what factor covered in Section III.C. (a) is designed to address. That section "access rights to customer information" could be misinterpreted to cover customer access to information rather that employee access to information. Since that is not the intent, a clarification would be helpful.

Community banks have told us, that while there is universal agreement on the importance of a policy on access to information, small institutions must approach access differently from large institutions. Some small financial institutions must be allowed significant leeway in determining each individual employee's level of customer information access. It is critical that financial institutions not be placed at a competitive disadvantage by limiting customer service because of limitations on employee access to customer data. There is a delicate balance between customer service and data security. We agree that it is inappropriate for employees to have access to customer data unrelated to their job function. However, many areas of the bank provide customer service to all customers of the bank (including loans, deposits, and customer names and addresses). Therefore a high level of access to customer data is necessary. Flexibility, once more, is key to a workable rule.

In addition, the factor covering encryption of electronic customer information should not cover all situations. Information security officers may reach the conclusion that encryption is not necessary in some instances and banks should be free to follow that professional advice. As with several of the other factors, language clarifying that these are suggestions would help alleviate concern with the potentially broad nature of the factors.

The proposal also seeks to have institutions consider appropriate " monitoring systems and procedures to detect actual and attempted attacks or intrusions into customer information systems." The aforementioned SARs already include, in the June 2000 revision, a new check box for so-called "computer intrusions" that must be filed with the Financial Crimes Enforcement Network (FinCEN). To avoid any confusion about the scope of a system covering computer intrusions, the guidelines should be consistent, perhaps by simply referring to this existing requirement. This is important because the new SAR form defines the act of computer intrusion and also describes what is not covered by this requirement (e.g. attempted intrusions of websites or other non-critical information systems of the institution that provide no access to institution or customer financial or other critical information). There is also no specific requirement to "monitor" systems but a known attempt cannot be ignored and must be reported.

Finally, the agencies invite comment on the "appropriate degree of independence" that should be specified when testing the information security system. The Bank Secrecy Act (31 USC 5311 et. seq.) created a testing requirement for internal review and permits the use of bank personnel or outside parties. Institutions simply must ensure that someone outside of the BSA compliance area conducts the review. The information security review should be handled in the same manner.

8. **Outsourcing Arrangements**

Exercising due diligence in managing outsourcing arrangements is another critical element in an information security program, but it is difficult to determine whether a service provider has actually implemented an effective information security program. The proposed guidelines should establish that obtaining and reviewing the program is adequate; however a financial institution should not be required to review the internal systems and implementation processes of a third-party provider.

The proposed guidelines should specifically state that obtaining and reviewing a third-party information security program is sufficient. Financial institutions should not be required to perform in-depth reviews and analyses of third-party provider systems and recordkeeping. Further, unless the guidelines provide further guidance on what is considered "appropriate due diligence", the definition will be left open to interpretation by banks and regulators and could result in examination and enforcement inconsistencies throughout the industry. It would be helpful to state in any final guidelines that the degree of due diligence should appropriately depend on the sensitivity of information to which the third party has access.

**Summary**

As the industry prepares for full compliance with the overall privacy provisions under Gramm-Leach-Bliley, we recognize the importance of having the consumer fully understand our commitment to protecting the security and confidentiality of their information. The industry has worked diligently in the information security area over the years and the assistance of the banking agencies in these efforts has been extremely helpful. We urge the agencies to continue to offer advice and guidance on a regular basis and we remain ready to assist the government in this area.

Thank you for the opportunity to present our views. If you have any questions or need additional information, please feel free to contact me at (202) 663-5029.

Sincerely,

John J. Byrne