WISCONSIN
BANKERS
ASSOCIATION

48434.pdf

(27)

August 25, 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 Wisconsin Bankers Association (WBA) is the largest financial institution trade association in Wisconsin and represents nearly 400 state and nationally chartered banks, savings and loan associations, and savings banks located in communities throughout the state. WBA appreciates the opportunity to comment on the proposed rule issued by the Federal Reserve Board, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision ("the Agencies"), which would 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.

4721 SOUTH BILTMORE LANE
MADISON, WI 53718

P.O. BOX 8880
MADISON, WI 53708-8880

608-441-1200
FAX 608-661-9381

www.wibank.com

Financial Institutions Already Have Strong , Effective Security Policies and Procedures to Protect and Prevent Unauthorized Access to Customer Information, Thus the Agencies Should Only Develop Guidelines that are Flexible.

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] Furthermore, it is well known that financial institutions maintain, and require their employees to adhere to, strict policies of confidentiality regarding customer information. In fact, it is extremely common for institutions to use as grounds for immediate termination, an employee's breach of such policies. Hence, it is clear that all institutions already have policies and procedures regarding the protection of customer information. Therefore, WBA believes that the Agencies should only continue to develop guidelines that provide a great degree of flexibility rather than the rigidity of a regulation to address this important area.

The Standards for Safeguarding Customer Information Should be Issued as Guidelines and Not as Regulations.

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. WBA believes 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. Therefore, WBA urges the Agencies to consider several modifications to this proposal and issue the final product as guidelines.

Because Community Banks Have Limited Resources, the Guidelines Should Permit Such Institutions to Continue to Use Existing Information Security Policies and Procedures Without Amendment.

The Agencies seek comment on the impact of this proposal on community banks. Given the fact that community banks most often operate with limited resources and personnel, it remains imperative that any final Guidelines allow community banks

[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.

the flexibility to continue using their existing information security programs in their current format. According to a member of the financial services industry, "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." In fact, many if not all, community banks would experience undue burden if required to eliminate existing and already effective information security procedures to create an entirely new program simply because of the implementation of the Guidelines. Therefore, WBA urges the Agencies to build into the Guidelines flexibility for community banks and institutions.

The Guidelines' Definition of "Customer" Should Be Consistent with Regulation P's Definition and Should Not Be Broadened to Include All Consumers or Business Customers.

Section 501 of Gramm-Leach-Bliley refers to "customer" information. The Agencies have interpreted "customer" in Regulation P as a consumer with whom the institution has a continuing relationship such that the institution provides to the consumer one or more financial products or services that are to be used for personal, family or household purposes. Clearly, this definition does not include all consumers, nor does it include any business customers. Thus, only information and records regarding customers, as that term is used in Gramm-Leach-Bliley and as interpreted in Regulation P, should be covered by the Guidelines. In addition, there is no policy reason to expand the definition for purposes of an institution's security program nor is there a policy reason for the imposition of additional costs that such change would invariably create. For these reasons, WBA strongly urges the Agencies not to go beyond the scope of the proposed Guidelines and cover records of all consumers and business clients.

"Customer Inconvenience" Should be Eliminated From the Objectives Set Forth in the Guidelines.

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.

The Level of Involvement of the Institution's Board of Directors Regarding the Specific Provisions of its Information Security Program Should be Left to the Institution's Discretion.

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."

WBA agrees with the need to have security programs supervised at high levels of the institution but believes 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.

Institutions Should Have Discretion to Determine the Frequency that Information Security Program Reports are Given to Boards of Directors.

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 reports to the board. For example, material information should be reported more frequently that routine information.

In addition, community bankers have indicated that due to their limited resources, 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.

The Guidelines Should Clarify that the Factors an Institution Should Consider in Evaluating an Information Security Program are Merely Suggestions and Not Requirements.

The proposed Guidelines also list a number of factors that an institution "should" consider in evaluating program adequacy. While WBA recognizes this proposal is

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

drafted as guidance to the industry, it urges 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."

The Guidelines Should Provide Institutions with a Great Degree of Flexibility Regarding Which Employees May Access Customer Information.

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. WBA agrees 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 Guidelines Regarding Monitoring Systems and Procedures to Detect Intrusions of Customer Information Systems Should Be Consistent with Those Already Addressed in the Bank Secrecy Act.

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.

The Guidelines Should Not Require Financial Institutions to Review the Internal Systems and Implementation Processes of Third-Party Service Providers.

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.

The Agencies Should Not Issue Guidelines Until a Reasonable Period of Time Beyond the Date of Mandatory Compliance with Regulation P has Elapsed.

Currently, financial institutions are diligently working to devise the privacy policies and notices they are required to provide by July 1, 2001. Without question, the Agencies must understand that this task is of monumental proportion for many institutions. In fact, institutions are devoting a great deal of time, resources and personnel to achieve well-written privacy policies within the mandatory date of compliance. To impose on institutions the additional task of creating customer information security programs concurrently with the creation of privacy policies would require such institutions to divide their precious and limited resources still further. WBA urges the Agencies not to place institutions in this position. WBA

believes a more workable approach to the issuance of Guidelines would be to permit a reasonable period of time (12-18 months) to pass beyond July 1, 2001 before such issuance occurs.

Rescission of Y2K Standards for Safety and Soundness Is Appropriate.

WBA agrees with the Agencies' decision to rescind the Year 2000 Safety and Soundness Guidelines for obvious reasons.

Conclusion.

As the industry prepares for full compliance with the overall privacy provisions under Gramm-Leach-Bliley, WBA recognizes the importance of having the financial institution customers fully understand the industry's 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. WBA urge the Agencies to continue to offer advice and guidance on a regular basis.

Again, WBA appreciates the opportunity to comment on this proposal.

Sincerely,

Harry J. Argue
Executive Vice President/CEO