48443.pdf

35

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]

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

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]

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

Subject: *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:

The Massachusetts Bankers Association (Association) which represents more than 200 commercial savings, and co-operative banks and savings and loan associations with $300 billion in assets would like to thank the Agencies for the opportunity to comment on the proposal to implement sections 501 and 505(b) of the Gramm-Leach-Bliley Act (GLB). Section 501 requires the banking agencies to establish appropriate standards relating to administrative, technical, and physical safeguards for customer records and information.

Under the proposal, each financial institution would be required to create, implement, and maintain a comprehensive information security program that would identify potential risk to the security of customer information, as well as establish a written plan which safeguards customer information. Each plan must be tested and periodically adjusted to account for changes in technology, business arrangements or threats to information security. Additionally, each institution's program must be approved and overseen by its board of directors.

Financial institutions have a long history of protecting customer privacy. In 1997, the industry formally adopted privacy principles which emphasized the development of policies to protect customer information. Last year, the Association conducted a member survey of our Consumer Privacy Task Force that showed that all the respondents have formal practices and procedures in place to safeguard customer information, and the nature and scope of polices and practices varied greatly depending on the complexity and size of the institution. For this reason, it is important that the agencies' standards contain maximum flexibility for adaptation to different financial institutions' practices and needs.

As a trade association that represents a significant number of small community banks, we commend the agencies sensitivity to the impact of the proposal on community banks. We believe that the proposed guidelines will provide a useful framework for evaluating whether these institutions are appropriately safeguarding customer information. We support the guidelines but believe that the Agencies should clarify certain aspects of the proposal in the final rule as indicated below.

The following are topics or questions raised in the preamble and other sections of the proposal.

1. *Should the final standards be Regulations or Guidelines?*

   Section 501 of title V of GLB does not mandate that the standards for protection of nonpublic personal information be issued as regulations. The industry has established effective policies in security and confidentiality of customer information and is working to make sure that these policies remain current as technology changes. We strongly believe that the standards for safeguarding consumer information should be as Congress intended, issued in the form of guidelines. We are concerned that the issuance of regulations would burden financial institutions with a number of technical violations unrelated to the effectiveness of an institution's policy.

   However, the agencies could provide help to community banks by identifying minimum standards for small institutions, as well as some guidance as to the maximum limits expected by the agencies. Without such general parameters, community banks will be unable to accurately measure the effectiveness of their policies and procedures or how to meet the requirements of the guidelines.

2. *What is* the *Impact of the Proposed Guidelines on Community Banks?*

   Due to limited resources, many community banks outsource a number of bank functions or operations with third parties rather than operate these functions in-house. The proposed guidelines should not place these banks at a competitive disadvantage or a greater compliance burden as a result of these arrangements. Many have already addressed security hazards and threats to customer information. These banks should be allowed to continue in their current practices and procedures without having to dismantle and incur the cost of creating another control system in compliance with these guidelines.

3. Factors for Risk Assessment and Risk Management

   Clarification is needed with respect to risk management proposed paragraph III.C. Some factors are confusing; for example factors (a), (c), and (d) should provide examples and parameters for compliance. Factor (f) requires a background check on individuals with access to customer information, which could prove costly for small banks since their employees often function in many capacities all could have access to customer information in order to provide a high level of customer service. It is important to recognize that these institutions must find an appropriate balance between customer service and data security. Factor (h) refers to monitoring systems to detect actual or *attempted* attacks or intrusions into computer systems. There should not be a specific requirement to continuously monitor systems for possible intrusion. While we agree that intrusions should be reported and addressed, it is unreasonable to expect community banks to monitor for attempted intrusions since their systems would most likely need to be upgraded for this capability. Furthermore, if these standards become regulations, then institutions will need clear examples of how compliance can be met under the factors listed in the paragraph.

The agencies invite comment on the degree of independence that should be specified when testing the information security system. The guidelines should state that a person independent of those who conducted the test should verify the information security program. A requirement that the review be conducted by an independent third party would be particularly burdensome to smaller community banks.

For the reasons described above, we believe that the proposed standards for developing a risk management plan may be unreasonable and overly burdensome for many community banks. We suggest that the agencies develop a more simplified standard for smaller institutions.

4. Definition of "*Customer*"

Including businesses in the definition of "consumer" goes beyond the scope and intent of GLB. Section 501 of GLB refers to "customer" information, which does *not* include business customers. Personal consumer information unlike business information carries an extremely high degree of "sensitivity" to confidentiality. The inclusion of businesses in the definition of "customer" could greatly increase the compliance burden and cost to all institutions. We strongly oppose the inclusion of an expanded definition as part of the guidelines.

5. Rescission of Y2K Standards for Safety and Soundness

We believe that it would be appropriate at this time for the Agencies to rescind the Year 2000 Safety and Soundness Guidelines.

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 that the board would 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."

While the board may approve security programs supervised at high levels of the institution, the board should have the discretion to delegate authority to senior management or executive officers for oversight of the security program. In fact, the degree of board involvement in an institution's information security program should be determined by the business strategy and practices 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.

7. Reporting Frequency

Given the limited resources of community banks, an appropriate reporting frequency would be annually or on an as needed basis, dependent upon changes that affect the plan. For example, the board could schedule an additional meeting when changes in technology or the bank's structure pose a threat to the security of customer information. We believe that it is extremely important that each institution have the flexibility to determine the appropriate reporting frequency required.

8. Outsourcing Arrangements

The Agencies have requested comment on how the guidelines should address the appropriate treatment and oversight of outsourcing arrangements. Presently financial institutions include confidentially clauses in contracts with third-party providers. Beyond due diligence, institutions should not be required to ensure that the vendor 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 liable for the internal systems and implementation processes of a third-party provider. Any guidelines should model the final rule for "Privacy of Consumer Financial Information." The final guidelines should clearly specify what will be considered "appropriate due diligence" to avoid misinterpretation.

In closing, one of the hallmarks of the industry is customer confidence in the bank's ability to properly safeguard and protect personal information. Financial institutions fully understand the importance of protecting the security and confidentiality of customer records and look forward to the agencies guidance in this area.

Thank you for the opportunity to present our comments on this proposal. If you have any questions or need additional information, please contact me at (617) 523-7595.

Sincerely,

Tanya M. Duncan
Director, Federal Regulatory and Legislative Policy

Tanya\corres\comnt00\safecustinfo.doc