48423.pdf

(16)

California Bankers Association
Established 1891

August 25, 2000

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

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

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

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

Re: Protection of Customer Information

Dear Sir/Madam:

The California Bankers Association is a nonprofit professional association incorporated in California, and represents commercial banks and savings and loans (hereafter, simply "banks") in the state. CBA regularly solicits comments from its members for submission to banking agencies on matters of importance to the banking industry. Protecting the confidentiality and security of customer information is such a matter.

Despite the recent legislative and public focus on the privacy of consumer financial information, depository institutions hold and always have held an exemplary record of

maintaining the confidence of their customers. Even in the absence of explicit regulatory guidelines, the protection of consumer information has ever been a top priority of every bank. The industry understands that any compromise of data integrity could adversely affect customer relations, expose banks to legal liability, and result in direct monetary losses.

Guidelines v. regulations. Neither industry experience nor the intent of Section 505(b) of the Gramm-Leach-Bliley Act ("GLB Act") warrants the imposition of formal regulations. Neither Congress nor the agencies have suggested that industry standards and practices are deficient. CBA strongly requests that the agencies adopt high level guidelines rather than another regulation, and apply a light hand to supervision unless and until the emergence of actual risks justify a more aggressive approach. If an individual institution's missteps pose a threat to its safety and soundness or to its customers' privacy, bank supervisors already have ample authority to take appropriate actions.

The protection of customer information is not a field that is ripe for aggressive regulatory supervision. In principle, the proposal reflects policies and practices already in place. In our view, the proposal adds great value in recommending uniform elements of a program. The agencies correctly note that no single model can be used by different institutions; therefore, the guidelines of necessity should be general. In contrast, the issuance of regulations accompanied by detailed examination procedures would do little more than increase compliance costs and open the door to technical violations.

Board supervision. We believe it is consistent with business practice that responsibility over data integrity and protection is delegated to senior management. As a general rule it is the duty of the board to provide high level direction to the bank rather than run it. CBA has found it necessary over the years to resist the regulatory reflex to deluge ministerial duties upon largely voluntary bank boards which, for good reasons, often include non-bankers. In addition to carrying out customary corporate governance, a bank board by regulation is already obliged to oversee a host of other matters ranging from banks' camera systems (Federal Reserve's Regulation H) to the filing of each and every suspicious activity report (BSA). To saddle bank boards with yet another specific task that could be overseen by senior management is a nonproductive exercise, and may even expose board members to greater liability under the director's duty of care.

For these reasons, we disagree that a board should "oversee efforts to develop, implement, and maintain an effective information security program." These duties are properly delegable. On the whole, we agree with the proposed duties set forth in Section III.A.2. for bank management, except that the management's report to the board should be streamlined by deleting everything after "Report to the board on the overall status of the information security program."

Oversight of service providers. We agree that banks' contractual third parties should not be instruments of breaching consumer privacy. Nevertheless, CBA objects in the strongest terms any requirement to exercise "due diligence in managing and monitoring outsourcing arrangements" to confirm that service providers' protection programs are "consistent with these Guidelines."

The proposed duties would be onerous and expensive. Banks rely on numerous contractors, from messengers to mainframe service providers, that handle customer information. It is not practicable for a bank to ensure that each contractor regularly reports to its own board about information security and that each has met the host of other standards listed in the proposal. Also, community banks in particular would find it extremely difficult to monitor major service providers with whom they have little or no bargaining power.

More critically, a duty to monitor would increase the likelihood that a bank would be joined in any civil action arising from the actions of its contract party. The GLB Act cannot be reasonably construed to demand such a result, and we believe the risks are sufficient to warrant either elimination of this provision or clarification.

Other issues. The guidelines should remain within the scope of Section 501 of the GLB Act, which covers only consumers and not business customers. Regardless of the merits of covering all customer information or the practical implications of segregating policies, we believe the agencies simply do not have the statutory authority under the GLB Act to include business customer information within the proposal.

Of course, we agree with the decision to rescind the Year 2000 Safety and Soundness Guidelines. We commend the agencies for the leadership they provided not only to the banking industry but to other business sectors as well.

CBA appreciates this opportunity to submit its comments. We appreciate the agencies' efforts in identifying the elements of an information security program. We suggest that the guidelines are issued simply as suggestions rather than mandatory elements in each bank's program. If you have any questions, please do not hesitate to contact me.

Sincerely,

Leland Chan
Associate General Counsel