48436.pdf

29

MBNA AMERICA

Joseph R. Crouse
Senior Executive Vice President
Legislative Counsel

MBNA America Bank, N.A.
Wilmington, Delaware 19884-0127

(302) 432-0716

2000 AUG 25 P 2:49

August 25, 2000

VIA UPS Overnight Delivery

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

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

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

Manager, Dissemination Branch
Information Management
and Services Division
Office of Thrift Supervision
1700 G Street, NW
Washington, D.C. 20552

Ladies and Gentlemen:

This is the comment letter of MBNA America Bank, N.A. ("MBNA") regarding the Joint Notice of Proposed Rule Making on the Proposed Guidelines for Establishing Standards for Safeguarding Customer Information published in the Federal Register on June 26, 2000 (Volume 65, No. 123, Pages 39472 – 39489) by the Office of the Comptroller of the Currency ("OCC"), the Board of Governors of the Federal Reserve System ("FRB"), the Federal Deposit Insurance Corporation ("FDIC") and the Office of Thrift Supervision ("OTS") (collectively, the "Agencies"). We refer to the proposed guidelines of the Agencies, which implement Sections 501 and 505(b) of the Gramm-Leach-Bliley Act ("GLBA"), as the "Proposed Guideline". While MBNA's primary regulator is the OCC, we and our affiliates also are subject to regulation by the FRB and the FDIC and we provide this letter to the Agencies because of the common issues involved and our desire for uniformity when final adoption occurs (the "Final Guideline").

MBNA is one of the world's largest issuers of MasterCard and Visa brand credit cards with approximately 21 million Customers in the United States. In business for 18 years and listed on the New York Stock Exchange since 1991, our managed loan outstandings at December 31, 1999

were $72.3 billion and our earnings for 1999 were $1.024 billion. Co-branding relationships, where MBNA provides credit card and other financial products and services to members of a group sharing common interests or to customers of other financial institutions or commercial organizations, are an integral part of our business. Worldwide, MBNA's products are endorsed by more than 4,500 organizations. In addition to credit cards, together with our affiliates we offer consumer deposits, consumer finance, insurance and travel products. Our products and services are sold and serviced almost entirely over the telephone and through the mail, although the Internet is an increasingly important channel.

Our primary concerns with the Proposed Guideline are: (i) sufficient regulatory guidance and oversight already exist to assure appropriate administrative, technical and physical safeguards for customer records and information; (ii) management discretion in tailoring information security must be preserved; (iii) establishing a Final Guideline for something as dynamic as security procedures may actually adversely affect the safeguarding of customer records and information if financial institutions work only to meet mandated items; and (iv) given a choice between a Final Guideline and a final rule, we prefer a Final Guideline because it is more flexible and better accommodates constantly changing security risks and the widely different capabilities and priorities of various financial institutions in addressing them.

Our comments follow the Section-by-Section Analysis of the Proposed Guideline.

I.C.2 Customer Information

We recognize that the Proposed Guideline defines "Customer" consistent with the Agencies' privacy rules published in accordance with the GLBA (the "Privacy Rule"). As a practical matter at the institutional level, any information security program should be established and executed for all of a financial institution's records – not just customer information. Effective security control over all aspects of the financial institution's records, systems, and facilities contributes to safety and soundness. Nevertheless, the Final Guidelines should provide sufficient latitude for variations in security programs, suited to the different needs of different business lines, and, in particular, as in the Proposed Guideline, should be directed exclusively at the establishment of guidelines for only "nonpublic personal information about individuals who obtain financial products for personal, family or household purposes," not business purposes.

III.A Involve the Board of Directors and Management

MBNA Management acknowledges and consistently meets its responsibility to establish and maintain an effective control environment, including an effective security program. MBNA's Board of Directors regularly receives information concerning the effectiveness of the security program through the results of both internal and external audits, numerous regulatory examinations, and the minutes from standing Risk Management Committee meetings. We note this as evidence supporting the OCC's statement regarding the *Unfunded Mandates Act of 1995*, "The OCC believes that most institutions have already established an information security program because it is a sound business practice that also has been addressed in existing

supervisory guidance". That is, institutions have fashioned policies to fit the needs of their own business lines and customers.

The flexibility for management to exercise discretion in the continuing evolution of each institution's security needs must be preserved in the Final Guidelines. The Board of Directors and Management must have accountability, and must also have the authority to shape policy, perhaps guided, but not displaced by, government pronouncements.

III.B Assess Risk

Assessing the risks that threaten the security, confidentiality, or integrity of financial institution records and customer information is an ongoing effort – not a point in time exercise. The risk assessment process is a fundamental component of every effective security program. The Proposed Guideline's value is limited if the risk assessment process is proposed as a separate, point-in-time exercise. As noted above, if the Final Guideline requires a separate set of best practices, the information security of a bank could deteriorate over time through management to the regulatory requirements as opposed to performing ongoing assessments and devising reactions to potential threats. Given the rapid pace of technology and business changes, banks need the flexibility to adapt to a changing environment.

III.C Manage and Control Risk

The proposed security practices listed in this section of the Proposed Guideline are but a subset of the entire population of control activities potentially required to properly manage the risk involved. Given constant changes in information technology, information security practices must also change constantly. Safety and soundness is not enhanced, and in fact may actually be impaired, by listing a mere subset of control activities. Discretion in choosing among alternatives should remain within management's discretion.

For example, financial institutions must be free to engage either internal or external security professionals as appropriate, in management's judgment, to provide the expertise on the specific security practices relevant to the risk involved. The degree of independence over testing of information security systems should be similar to the degree of independence over the testing of any other internal control process. MBNA is confident that its Internal Audit Department provides the necessary independence and produces a more thorough review because of its familiarity with existing systems, procedures and personnel. Any company will, as prudence dictates, contract for services with external consultants when it lacks the requisite expertise, or has only temporary needs. Requiring tests to be conducted by external consultants imposes unnecessary financial burdens on financial institutions. We believe management should decide when contracting with a third party is required. The current regulatory guidelines governing independence, competency, and scope of the audit function provide adequate safeguards to ensure effective testing.

III.D Oversee Outsourcing Arrangements

Existing financial institution vendor management responsibilities ensure proper oversight of security controls implemented by third parties to protect financial institution records and customer information. MBNA's vendor management program involves numerous components extending well beyond information security, including required contract provisions, explicit, quantifiable and measurable performance requirements and ongoing performance monitoring. Based upon our experience, existing regulatory oversight of vendor management programs is sufficient. Placing responsibility on financial institutions to conduct on-premises reviews or formal examinations, however, would be unduly burdensome. We advocate use of contractual provisions as the primary tool for financial institutions to provide assurances of vendor security.

III.E Implement the Standards

Requiring implementation of specific security practices (such as those listed in Section III.C) within mandated timeframes affects MBNA as follows:

(i) Encrypting all customer data (both at MBNA and with all third parties) is a substantial and unnecessary financial burden.

(ii) Expanding vendor management programs to incorporate onsite security evaluations of all third parties where customer data is shared is cost prohibitive and, in many instances, wasteful of corporate resources. MBNA agrees that onsite inspections of third parties processing large amounts of sensitive customer data may be warranted – but common sense and basic risk management strategies suggest flexibility in deciding the level of oversight required for third parties processing smaller amounts of data or data of less sensitivity.

(iii) Given the delay in publication of the Proposed Guideline, if specific security practices are mandated in the Final Guideline, an extension of the existing deadline (July 1, 2001) is required to implement policies, controls and staffing to ensure proper compliance.

MBNA appreciates this opportunity to provide comments on the Proposed Guideline. If you have any questions please contact the undersigned at 302-432-0716.

Sincerely,