48420

(13)

Gottlieb, Mary H

From: Hurwitz, Evelyn S on behalf of Public Info
Sent: Friday, August 25, 2000 4:54 PM
To: Gottlieb, Mary H
Subject: FW: DOCKET NO. 2000-15

-----Original Message-----
From: Charles Lee [mailto:Charles.Lee@midfirst.com]
Sent: Friday, August 25, 2000 3:58 PM
To: 'PUBLIC.INFO@OTS.TREAS.GOV'
Subject: DOCKET NO. 2000-15

Attached is MidFirst Bank's response to the request for comment on Customer Information Security proposal.

RESPONSE.doc

(13)

August 22, 2000

DOCKET NO: 2000-15

VIA FAX 202 906 7755
VIA E-MAIL PUBLIC.INFO@ OTS.TREAS.GOV

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

Manager,

This is in response to the Joint Notice of Proposed Rulemaking by the OTS and other banking agencies regarding customer information security. MidFirst Bank, Oklahoma City, Oklahoma, is pleased to have the opportunity to provide comments regarding the proposal.

- Frequency of Board Reporting - MidFirst concurs with the requirement to inform the Board of Directors regarding the information security program; however, MidFirst requests specific guidance within the final rule regarding the frequency of Board reporting of such matters. MidFirst opines that the final rule should read to the effect that "management should report the status of the information security program to the Board no less frequently than annually". This would require that the Board must be apprised of the adequacy of and compliance with the security program at least annually which is sufficient for the Board to identify the need for modification to the program. This approach also allows a more frequent reporting schedule at each Board's discretion. As such, it allows institutions to adapt their reporting based on their individual and unique circumstances and creates minimal regulatory burden. This would also correlate with the fact that external audits are performed annually and Board policies are typically approved annually. Further, most processes and systems relating to information security will not change materially from year to year thereby minimizing the testing and reporting frequency of such systems. MidFirst encourages the OTS to affirm that the testing and reporting can be flexible so that the same tests are not required year after year.

- Form of Report – MidFirst requests that the OTS specifically affirm that the format and content are at the Board's option and discretion. This would extend to oral as well as written reporting to the Board. Provided the Board is comfortable with the content and the format of the report, no other regulatory requirements regarding reporting should be imposed.

- Degree of Detail in Guidelines – MidFirst believes the listed factors for use in evaluating the adequacy of policies are reasonable; however, MidFirst also believes that any such listing in a final regulation should be illustrative in nature rather than prescriptive. The degree to which each of these factors is important will vary from institution to institution and in some cases may not be applicable at all. Further, in some cases, a single factor may so dominate an institution's operations that all other factors are immaterial. The Board of Directors of an institution is in the best position to determine the importance of these factors and the risk each factor poses to customer information security; as a result, regulation should not rigidly dictate the specific factors to be considered in the evaluation of information security policies.

- Training on Fraud Detection - The risk of fraud has not recently developed, and institutions have a long history of developing processes to detect fraud and to train employees in methods most likely to prevent fraud. Since fraud management practices are an integral component of an institution's daily operations and since the implementation of reasonable fraud management is in the institution's best interest, a specific requirement in the final rule regarding employee training in relation to fraud seems unnecessary.

- Independence of Testing - MidFirst opines that the level of independence required for testing of compliance with information security systems and the review of test results are best left to the determination of the Board and management. Further, MidFirst opines that the types and the frequency of such testing are also best left to the Board and to management. Such testing processes and the test results will be subject to regulatory examination and audit which provides regulators with a means of detecting clearly inappropriate testing processes; however, by providing the Board with this flexibility, the testing process that is most reasonable for each institution can be implemented. The testing program and its frequency are not solely calendar dependent, but also should incorporate elements relating to experience level of employees, newly implemented systems, previous testing results, and environmental conditions. Establishing a testing frequency in the final rule will preclude the Board from reaching the appropriate balance between testing scope, frequency, cost, and benefit given the institution's unique operating environment. MidFirst also encourages the OTS to affirm that the Board and those with responsibility for testing should have the flexibility to modify scope to focus on areas of interest or concern and not merely to perform the same scope and same procedures on a repetitive basis.

  MidFirst also opines that the Board and management are in the best position to determine whether independent third party testing is required or whether the testing can be performed in-house; MidFirst opposes any requirement for testing to be performed only by third parties. MidFirst also suggests that it is permissible for such testing to be incorporated into external audits. By allowing this flexibility, the Board will be able to best control the costs associated with the required testing and will be able to select the most effective means of testing. Mandating the use of third party testing reduces management's options in employing in-house expertise, precludes management from utilizing judgment relating to the options best suited to the institution, and reduces options relating to cost minimization strategies.

- Outsourcing - MidFirst supports a final rule that would allow an institution to rely upon contractual provisions, certifications, or statements by third party service providers and vendors relating to compliance with prudent industry best practice in the management of nonpublic customer information. Contracts routinely contain representations and warranties regarding operations and conditions of the parties or require management to certify as to certain facts; extending representations and warranties or management certifications to information security is not unreasonable or without precedent. A third party agreeing to comply with the best practices relating to an information security system offers the most reasonable basis for an institution to believe compliance with this proposed rule is achieved. MidFirst does not support a requirement for an institution to test a third party's information security practices and procedures.

If additional information on any of the above topics is needed, please contact the undersigned.

Sincerely,

Charles R. Lee
Vice President
MidFirst Bank
PO Box 26750
Oklahoma City, OK 73126
405 840 7600