

48424.pdf

17

Gottlieb, Mary H

From: Hurwitz, Evelyn S on behalf of Public Info
Sent: Friday, August 25, 2000 4:53 PM
To: Gottlieb, Mary H
Subject: FW: Comment on Proposed Security Sstandards for Customer Information



ATT14521.txt



Adobe Portable

Document

-----Original Message-----

From: james.keller@pncbank.com [mailto:james.keller@pncbank.com]
Sent: Friday, August 25, 2000 4:11 PM
To: regs.comments@federalreserve.gov; public.info@ots.treas.gov;
regs.comments@occ.treas.gov; comments@fdic.gov
Subject: Comment on Proposed Security Sstandards for Customer
Information

***** Virus Scan Message (on vwall2-new)

GLB comment letter customer information security.PDF is scanned and no
virus found

Attached in Adobe Acrobat format is PNC's comment on the Proposed Security Standards for Customer Information. If you have any questions, I can be reached at the above e-mail address or 412-768-4251.

Jim Keller

(See attached file: GLB comment letter customer information security.PDF)

17

The PNC Financial Services Group, Inc.
249 Fifth Avenue
One PNC Plaza, 21st Floor
Pittsburgh, PA 15222-2707

412 768-4251 Tel
412 762-5920 Fax
james.keller@pncbank.com

James S. Keller
Chief Regulatory Counsel

August 25, 2000

Via e-mail

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

Robert E. Feldman, Exec. Secretary
Comment/OES
Federal Deposit Insurance Corp.
550 17th Street, NW
Washington, DC 20429

Office of the Comptroller of the Currency
250 E Street, SW
Washington, DC 20219
Docket No. 00-13

Manager, Dissemination Branch
Information Mgmt. & Services Div.
Office of Thrift Supervision
1700 G Street, NW
Washington, DC 20552

Re: Proposed Customer Information Security Standards

Ladies and Gentlemen:

The PNC Financial Services Group, Inc. ("PNC"), Pittsburgh, Pennsylvania, appreciates the opportunity to comment to the federal financial institution regulatory agencies ("Agencies") on the proposed Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness ("Guidelines") (65 Fed. Reg. 39,472 (2000)), which the Agencies are issuing to implement Sections 501 and 505(b) of the Gramm-Leach-Bliley Act ("Act").

PNC is one of the largest diversified financial organizations in the United States, with \$75.7 billion in assets as of June 30, 2000. Its major businesses include regional banking, corporate banking, real estate finance, asset-based lending, asset management, global funds services and mortgage banking. PNC's full-service subsidiary banks have offices in Delaware, Indiana, Kentucky, New Jersey, Ohio and Pennsylvania. Through its federal savings bank and mortgage banking subsidiaries, PNC engages in retail banking activities nationwide.

This letter responds to the Agencies' specific requests for comment and identifies other issues of concern to PNC.

BACKGROUND ISSUES

In the Supplementary Information issued with the proposed Guidelines, the Agencies request comment on two general matters:

RESCISSION OF YEAR 2000 STANDARDS FOR SAFETY AND SOUNDNESS:

Comment Requested: The Agencies propose to rescind the Year 2000 Guidelines because the Agencies have concluded that since the events for which the Year 2000 Guidelines were issued have passed, the Year 2000 Guidelines are no longer necessary. The Agencies have requested comment as to whether rescission is appropriate.

PNC Response: PNC concurs that rescission of the Year 2000 Standards for Safety and Soundness is appropriate at this time.

FORM OF THE FINAL STANDARDS

Comment Requested: The Agencies have solicited comment on whether the final standards should be issued in the form of guidelines or regulations.

PNC Response: PNC recommends that the final standards be issued in the form of guidelines.

SECTION-BY-SECTION ANALYSIS OF THE PROPOSED GUIDELINES

I. Introduction

I.A. Scope of the Proposed Guidelines

Section I.A. of the proposed Guidelines states that the Guidelines apply to “customer information” maintained by or on behalf of the entities over which the respective Agencies have regulatory authority. Section I.C.3. proposes to define “customer” as any customer of a financial institution as the term “customer” is defined in Section __.3(h) of the Privacy Regulation implementing Title V of the Act. Section __.3(h) defines “customer” as a “consumer” who has a customer relationship with a financial institution.

Comment Requested: While the Agencies have proposed limiting the scope of the Guidelines to “customers” as defined by the Privacy Regulation, they have solicited comment as to whether a broader definition to include “records regarding all consumers, the institution’s consumer and business clients, or all of an institution’s records” would change the information security program that an institution would implement.

PNC Response: PNC recommends that the term “customer” in the proposed Guidelines be limited to customers as that term is defined in Section __.3(h) of the Privacy Regulation. Title V of the Act seeks to protect the nonpublic personal information of consumers. Section 501(b) of the Act requires the Agencies to establish appropriate standards “relating to the administrative, technical and physical safeguards” to ensure the “security and confidentiality of customer information.” (Emphasis added.) Since the statutory authority is limited to consumer customer information, we believe that the scope of the Guidelines should so be limited. The potential adoption of a broader definition of “customer” for purposes of implementing a financial institution’s information security program should not influence the regulatory definition.

II. Standards for Safeguarding Customer Information

II.B. Objectives

Section II.B. of the proposed Guidelines generally sets out the statutory objectives for a financial institution’s customer information security program that are found in the Act. Title V, Section 501(b) of the Act provides that each agency is to establish “appropriate standards” relating to “administrative, technical, and physical safeguards – (1) to insure the security and confidentiality of customer information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.” The Agencies have added protection against unauthorized access or use that could pose a “risk to the safety and soundness” of the financial institution.

Comment Requested: The Agencies request comment on whether there are additional or alternative objectives that should be included in the Guidelines.

PNC Response: PNC recommends that the Agencies use the authority granted to them by Section 501(b) to issue “appropriate standards” to modify the objectives set out in the proposed Guidelines. For example, we recommend that the phrase “designed to” precede any enumeration of objectives for a financial institution’s customer information security program. No security program can absolutely guarantee the security of customer information. Financial institutions should not be given an unachievable standard. An information security program should be “designed to” protect customer information. Additionally, we suggest the word “any” that precedes “anticipated threats or hazards” be deleted from item (2). It is not possible to protect against “any” anticipated threats. Some threats, such as a national emergency, may be beyond any one institution’s capabilities to protect against.

Further, we recommend that the word “inconvenience” be deleted entirely from item (3). Inconvenience is at best a subjective term. A more appropriate standard for item (3) is to protect

against unauthorized access that could result in substantial harm to customers or in risks to the safety and soundness of the financial institution.

III. Development and Implementation of Information Security Program

III.A. Involve the Board of Directors and Management

Proposed Section III.A. sets out the respective responsibilities of a financial institution's directors and management with respect to the Guidelines. The board's proposed responsibilities are to: (1) approve the institution's written information security policy and program; and (2) oversee efforts to develop, implement and maintain an effective information security program. Management's responsibilities are to: (1) evaluate the impact on the program of changing business arrangements (such as, mergers, alliances and joint ventures, and outsourcing arrangements), and changes to customer information systems; (2) document compliance with the Guidelines; and (3) keep the board informed of the overall status of the institution's information security program.

Comment Requested: The Agencies have invited comment on the appropriate frequency of reports to the board: whether the Guidelines should specify monthly, quarterly or annual reports. The Agencies have also asked whether the Guidelines should require the board to appoint a Corporate Information Security Officer or other responsible individual who would have the authority, subject to the board's approval, to develop and administer the institution's information security program.

PNC Response: While PNC recognizes that a board of directors should retain ultimate oversight responsibility of a financial institution's information security program, we believe that the frequency of such involvement, as well as the mechanism for discharging it, should be left up to the financial institution. Some institutions may believe a board committee, such as an audit committee, could better manage this responsibility because internal control matters may be addressed in more depth by a committee than by the full board. Other institutions may view board involvement as analogous to existing board responsibilities in such areas as Bank Secrecy Act compliance or more traditional security program oversight. Only by assessing its information security requirements in terms of its risks and infrastructure can a financial institution best determine the nature of its board involvement. The Guidelines should provide the flexibility for such determinations to be implemented by institutions as they deem necessary, subject to specific recommendations from their primary regulatory agency. While most large financial institutions have a position equivalent to Corporate Information Security Officer, we believe financial institutions should have the flexibility to administer their information security programs as they think best.

Accordingly, we suggest that Section III.A.1. be revised as follows: "The major responsibilities of the board in providing oversight of the institution's information security program are to: (1)

understand the institution's overall potential information security risk exposure; (2) approve the institution's overall information security risk tolerances, policies and program, and (3) periodically review and reevaluate the institution's overall information security risk exposure and the effectiveness of the program in managing risk. Such responsibilities may be fulfilled by a committee of the board, at the discretion of the financial institution."

Similarly, to provide financial institutions flexibility in managing their customer information security program, we recommend that Section III.A.2. be revised as follows: "The major responsibilities of senior management in providing oversight of the implementation of an information security program are to: (1) ensure that appropriate policies, processes, people, controls and risk monitoring systems are in place to sufficiently address security risk management objectives; (2) understand and give appropriate consideration to information security requirements in changing business arrangements (for example, mergers, alliances, and outsourcing arrangements); and (3) report to the board as appropriate regarding the overall status of the information security program, including, for example, material matters related to the following: risk assessments, risk management and control decisions; results of testing; attempted or actual security breaches or violations and responsive actions taken by management; and any recommendations for improvements in the information security program."

We believe that the frequency of such management reporting should be left to each financial institution as it deems appropriate.

III.B. Assess Risk

Proposed Section III.B. enumerates three steps in the risk assessment process: (1) identification and assessment of risks to security, confidentiality or integrity of customer information; (2) assessment of sufficiency of policies, procedures, systems, etc. to control risks; and (3) monitoring, evaluating, and adjusting risk assessment "in light of" changes in technology or sensitivity of customer information, and external threats to information security.

While the Agencies have not specifically requested comment on this section, PNC believes that each financial institution should have the discretion to determine its own risk assessment process and the elements for maintaining a reasonable control environment. If the current three-step process is retained, we suggest that the phrase "in light of" be replaced by "commensurate with."

III.C. Manage and Control Risk

Proposed Section III.C. describes the elements the Agencies suggest are required for a comprehensive risk management plan.

III.C.1. Elements

Paragraph III.C.1. lists eleven factors (a-k) that an institution “should” consider in establishing its policies and procedures.

Comment Requested: The Agencies have invited comment on the degree of detail that should be included in the Guidelines regarding the risk management program, which elements should be specified in the Guidelines, and any other components of a risk management program that should be included.

PNC Response: PNC believes that a detailed listing of the elements of a risk management program is not necessary. If, however, the Agencies choose to retain the listed elements (a-k), the introductory paragraph should clarify that these elements are only examples of elements to be included and not mandatory. This can be accomplished by replacing the last sentence of Section III.C.1. with a sentence that reads as follows: “Examples of policies and procedures each institution may consider are:”

More particularly, we recommend that Section III.C.1.d. on “Encryption” be revised as follows: “Appropriate encryption technologies should be used when transmitting customer information over un-trusted networks or un-trusted environments. Encryption is not always necessary when transmitting customer information”. Similarly, we recommend that Section III.C.1.f. be modified by the addition of the phrase “as appropriate” to the beginning so that revised Section III.C.1.f. would read: “As appropriate, dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information.” Dual control procedures and similar procedures are not always necessary.

III.C.2. Training

We suggest that Section III.C.2. be revised to read “Include in its information security program a training component designed to educate employees about prudent information security practices and the appropriate escalation of reporting of security incidents.”

III.C.3. Testing

The Agencies state in the introductory Section-by-Section Analysis that an information security program should also include “regular testing of systems to confirm that an institution and its service providers control identified risks and achieve the objectives to ensure the security and confidentiality of customer information.” The Agencies further state in proposed Section III.C.3. that test results should be “reviewed by independent third parties or staff independent of those who conducted the test.”

Comment Requested: The Agencies have requested comment on whether specific types of security tests, such as penetration tests or intrusion detection tests, should be required.

PNC Response: PNC believes that each financial institution should have the discretion to determine the types and frequency of tests appropriate to maintain a reasonable control environment.

Comment Requested: The Agencies have invited comment on the appropriate degree of independence that should be specified in the Guidelines in connection with the testing of information security systems and the review of test results. Should tests or reviews of tests be conducted by non-employees? If testing is done by employees, what measures, if any, are appropriate to assure their independence?

PNC Response: PNC agrees that an adequate information security program must include a testing or monitoring component to evaluate the adequacy of and adherence to the information security process. The identity of the persons conducting the testing or monitoring, whether independent third parties or internal staff, as well as the nature and depth of the process evaluation, should be based upon the information security risk assessments conducted by the institution. Tests or reviews of tests may be conducted by employees so long as the employees are independent of the process being tested.

III.D. Oversee Outsourcing Arrangements

In the introductory Section-by-Section Analysis of Section III.D., the Agencies state that a financial institution “should exercise appropriate due diligence in managing and monitoring its outsourcing arrangements to confirm that its service providers have implemented an effective information security program to protect customer information and customer information systems consistent with these Guidelines.”

Comment Requested: The Agencies have requested comment on the appropriate treatment of outsourcing arrangements and ask whether the Guidelines should contain specific contract provisions requiring service provider standards for customer information security.

PNC Response: PNC believes that very few service providers would permit outside parties to monitor their security information programs in a manner described in proposed Section III.D.

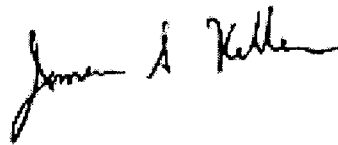
We believe that financial institutions should exercise care in choosing their service providers and in contractually obligating their service providers to implement and maintain an appropriate information security program. Financial institutions should not be required to verify compliance by service providers. Accordingly, we suggest that after the first sentence, the remainder of proposed Section III.D. be revised as follows: “A financial institution should exercise

appropriate due diligence in establishing its outsourcing arrangements so as to reasonably assure itself that its service providers have an information security program with basic elements that protect against unauthorized access and information misuse. A financial institution should contractually obligate a service provider to maintain the confidentiality of information provided to the service provider by the financial institution.”

CONCLUSION

PNC expresses its appreciation for this opportunity to comment on the proposed Guidelines. We hope our comments will be helpful to the Agencies in formulating the final Guidelines.

Sincerely,

A handwritten signature in black ink, appearing to read "James S. Keller". The signature is written in a cursive style with a long horizontal stroke at the end.

James S. Keller