4/84/32.pdf

25

Gottlieb, Mary H

From: Hurwitz, Evelyn S on behalf of Public Info
Sent: Monday, August 28, 2000 12:12 PM
To: Gottlieb, Mary H
Subject: FW: Comment on Proposed Regulation

clsscustinfo825.doc

-----Original Message-----
From: Chuck.Underwood@wachovia.com [mailto:Chuck.Underwood@wachovia.com]
Sent: Monday, August 28, 2000 12:12 PM
To: regs.comments@occ.treas.gov; regs.comments@federalreserve.gov; comments@fdic.gov; public.info@ots.treas.gov
Cc: Carl.Cowart@wachovia.com
Subject: Comment on Proposed Regulation

Federal Reserve Board -- Docket No. R-1073
Comptroller of the Currency -- Docket No. 00-13
Federal Deposit Insurance Corporation -- Comments/OES
Office of Thrift Supervision

Attached is a comment letter submitted on behalf of Wachovia Corporation and its subsidiary companies. This letter is in regard to the proposed Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness;
65 Federal Register No. 123: June 26, 2000..

The letter also is being delivered by regular mail.

Please contact Carl Cowart by e-mail at carl.cowart@wachovia.com or by phone at 336-732-7575 if you have any questions.

We appreciate the opportunity to participate in the regulatory rulemaking
process, and your acceptance of the attached comments.

(See attached file: clsscustinfo825.doc)

Wachovia Corporation
100 North Main Street
Winston-Salem, North Carolina 27150-3099

25

August 25, 2000

DELIVERED BY ELECTRONIC AND REGULAR MAIL

Ms. Jennifer J. Johnson
Secretary
Board of Governors of
the Federal Reserve Systems
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

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
1700 G Street, NW
Washington, D.C. 20552

Dear Sirs and Madams:

This comment letter is submitted on behalf of Wachovia Corporation and its subsidiary companies including: Wachovia Bank, N.A., Wachovia Operational Services Corporation, the First National Bank of Atlanta -Delaware d/b/a Wachovia Bank Card Services, and Atlantic Savings Bank, FSB (hereinafter collectively referred to as "Wachovia").

Wachovia Corporation is an interstate financial holding company with dual headquarters in Atlanta, Georgia and Winston-Salem, North Carolina, serving regional, national and international markets. Its member companies offer personal, corporate, trust and institutional financial services. Wachovia Bank, N.A., the principal subsidiary of Wachovia Corporation, has more than 700 offices and 1,300 ATMs in Florida, Georgia, North Carolina, South Carolina and Virginia.

Wachovia is pleased to respond to the joint notice of proposed rulemaking by The Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of Thrift Supervision, (collectively "the Agencies") on the proposed guidelines establishing standards for safeguarding customer information to implement sections 501 and 505(b) of the Gramm-Leach-Bliley Act ("the GLBA").

Section 501 of the GLBA requires the Agencies to establish appropriate standards relating to administrative, technical, and physical safeguards for customer records and information. These safeguards are intended to: insure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.

Wachovia appreciates the difficulty of crafting such guidelines and applauds the work of the Agencies in addressing these complex issues. Wachovia hopes that the comments, which follow, will be helpful to the Agencies as the final guidelines are developed.

Wachovia recommends that the final standards be issued in the form of guidelines as opposed to regulations. Guidelines would provide financial institutions flexibility in designing appropriate information security programs that reflect the risk environment of the institution. This should lead to more innovative, efficient approaches to information security that would benefit both the customer and the financial institution.

Scope of Guidelines

The Agencies have asked for comment on the definition of "customer" for purposes of these guidelines. Specifically, the Agencies have asked whether the scope of the guidelines should apply to records regarding all consumers, the institution's consumer and business clients, or all of an institution's records. The guidelines as currently worded clearly apply only to consumers and customers as those terms are defined within Title V of the GLBA. The statutory language is clear concerning the appropriate definition of "customer" and the recently issued Privacy regulation accurately reflects the statutory intent. Therefore, Wachovia recommends that all regulations or Guidelines issued pursuant to Title V of the GLBA should be consistent in scope. However, as a practical matter, Wachovia's information security program and practices do not distinguish between consumer and business customer information.

Board of Directors

The Agencies have specifically invited comment regarding the appropriate frequency of presenting the information security program reports to the Board of the financial institution. Wachovia believes that each institution should determine the appropriate reporting interval based upon the specific circumstances. We would recommend that instead of specifying required reporting to be monthly, quarterly or annually, that the appropriate wording should be "periodic reporting". Also the Guidelines should clarify that the Board, or a designated committee thereof, should "receive" reports but not have the primary responsibility of "overseeing" the effectiveness of an institution's information security program. The overseeing of the program should be the responsibility of an individual or management committee depending on the financial institution's specific risk factors.

Standards for Safeguarding Customer Information

Proposed paragraph II.B. describes the objectives for an information security program thusly: "A bank's information security program shall: 1. Ensure the security and confidentiality of customer information; 2. Protect against any anticipated threats or hazards to the security or integrity of such information; and 3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer or risk to the safety and soundness of the bank." Wachovia suggests that the use of the word "shall" in the objectives section is not appropriate for Guidelines. Rather, the following wording is recommended: "A bank's information security program should be designed to...". Also Wachovia recommends the following changes to this wording: replace "...any anticipated threats..." with "...any foreseeable threats..." and remove the word "inconvenience" from objective 3. This word is superfluous. Any threat that could result in "substantial harm" would surely be inconvenient.

Manage and Control Risk

Again, the word "shall" as used in this section is inappropriate. Wachovia favors the wording of section III.C. that is contained in the commentary, i.e., "...each institution should consider appropriate...". The specific elements of an information security program are subject to change due to technological advancements. It is essential that the Guidelines offer examples of elements and not

mandate the information security program "shall include" specific elements, which likely will change and thus become "dated".

Wachovia would suggest that the wording of the encryption element, III.C.d. be modified to reflect a focus on risk and Internet activity. The current wording is too broad and could be interpreted to apply to back-up files stored offsite. In addition, if information is on a public network, it cannot be controlled by a financial institution. Wachovia recommends that III.C.d. be changed to read "The appropriate use of encryption based on the level of risk."

The Agencies invite 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. Wachovia believes that the elements included in the Guidelines should be viewed as examples of prudent actions on the part of a financial institution in structuring an information security program. The actual components of an institution's information security program should reflect the risk environment of the institution. For this reason, we believe the level of detail in the proposed Guidelines is sufficient.

The Agencies request comment on whether specific types of security tests, such as penetration tests or intrusion detection tests, should be required. The security testing by a financial institution should reflect the complexity and nature of the business. A specific list of required types of testing is not advisable as this will most likely consistently change as technology and information storage practices change and develop. Therefore, the program should be enhanced as necessary based on the financial institution's needs/requirements and the changes in technology that impact the program. Furthermore, if these are guidelines, there should not be any "required" security tests.

The Agencies also have invited comment regarding 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. Specifically, the Agencies have asked if the tests should be conducted by persons who are not employees of the financial institution. Also, the Agencies have asked that if employees conduct the testing or review the test results what measures, if any, would be appropriate to assure their independence. Wachovia believes that financial institutions should have the flexibility to either have this testing done by employees or by external parties. Internal auditors have the necessary level of independence to test the information security system, and in most financial institutions they already do this. In fact the Office of the Comptroller of the Currency (the "OCC") has recognized the importance of independent auditors in monitoring the levels of technology risk within a financial institution. In OCC Bulletin 98-3, one finds the following wording: "Auditors provide an important control mechanism for detecting deficiencies and managing risks in the implementation of technology." Internal Auditors are uniquely qualified to perform independent testing of the institution's information security program in a cost-effective manner.

Wachovia recommends that the Guidelines should be modified to omit the requirement for independent third party verification of the results of the security tests. If these tests are conducted by an independent party (whether internal or external) verification would be both costly and unnecessary.

Oversee Outsourcing Arrangements

Wachovia believes that financial institutions are responsible for exercising appropriate due diligence in approving outsourcing arrangements and monitoring these arrangements to confirm that its technology service providers have implemented effective information security programs to protect customer information. The type of ongoing monitoring should be left to the discretion of the institution's Chief Information Officer, a committee overseeing the program or the internal audit department depending on the individual financial institution's structure.

Futhermore, Wachovia supports the use of a SAS 70 Report as one option for satisfying the ongoing due diligence requirements, but not as a requirement.

Wachovia would not be in favor of including within the Guidelines specific contract provisions requiring service provider performance standards in connection with the security of customer information. It has been Wachovia's experience that service-providers have been accommodating in accepting specific contract provisions regarding information security. It is appropriate that the Guidelines recommend that provisions regarding the protection of, security of and usage of customer information be included in all service provider contracts.

Critical services such as data processing, transaction handling, network services, software management, access controls, and contingency planning require minimum levels of controls in order to provide protection for customer information and their financial assets. The Agencies have asked if industry best practices are available regarding effective monitoring of service provider security precautions. The following is a listing of some basic components that could establish and or enhance the safeguarding of customer information:

- Policies and procedures that address risks and controls should be implemented to ensure the security of customer records and assets. These policies may include but not be limited to data center security, data security, network security/integrity, operations, contingency planning, and all third party alliances where customer information is stored or processed outside of an institution's corporate firewall.

    1. Data Center Security should include both physical and logical access controls that prevent unauthorized entry/access that would put at risk the confidentiality of customer information.
    2. Data security methodologies, including appropriate use of encryption that limit or prevent unauthorized access should be employed.
    3. Network security/integrity functions should be in place that proactively monitor network controls and detect network intrusions. There also should be physical and logical security policies that limit access to network infrastructure.
    4. Operations staff non-disclosure policies and agreements should be standard.
    5. Proactive contingency planning that minimizes risk due to loss or compromise of customer information should be in place.
    6. Controls over outsourced information and transaction processing activities should be equivalent to those that would be in place if the activity were conducted internally by the financial institution.

The above listing is not meant to be an exhaustive list of industry best practices but is reflective of the kinds of practices that a financial institution would hope to see in place within its chosen service providers. Although industry best practices exist, Wachovia does not recommend the use of current best practices in the Guidelines, as those practices will continuously change as technology and methodology develops.

Wachovia appreciates the opportunity to offer these comments to the Agencies and hopes that they will be helpful in formulating appropriate guidelines that meet the statutory intent of the GLB Act without placing an undue burden on financial institutions

Very truly yours,

(Signature of Jean E. Davis affixed to original copy)

Jean E. Davis
Senior Executive Vice President