48438.pdf

(31)

Edward G. Schwartz
AVP/Chief Information Security Officer
Office of Enterprise Information Security

August 24, 2000

Ms. 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

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

2000 AUG 25 P 2:49

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, D.C. 20552

Dear Sirs and Madams:

Nationwide appreciates the opportunity to comment to the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency and the Office of Thrift Supervision (collectively, "the agencies") on the proposed Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Recession of Year 2000 Standards for Safety and Soundness. As you may know, Nationwide is one of the largest insurance and financial services companies in the United States. Nationwide appreciates the work of the agencies in issuing the proposed rules and recognizes the challenges that the agencies face in addressing this complex issue. These comments are intended to provide constructive suggestions so that the final guidelines reflect appropriate business practices as well as the agencies statutory obligations.

GENERAL COMMENTS

Nationwide supports issuing the proposed guidance in the form of "Interagency Guidelines" rather than regulations. Promulgating guidelines rather than regulations will provide a greater degree of flexibility for financial institutions. This needed flexibility will promote greater innovation and advances in security procedures and practices that will, in turn, lead to greater protection of customer information.

SPECIFIC COMMENTS

Rescission of Year 2000 Standards

Nationwide agrees that rescission of the Year 2000 Standards for Safety and Soundness is appropriate at this time.

One Nationwide Plaza, 2-07-04
Columbus, OH 43215 2220

Tel 614 677 8651
Fax 614 677 8715
schware@nationwide.com

Nationwide Insurance
Nationwide Financial

Scope of Guidelines

The agencies invite comment on the scope of the guidelines. Nationwide urges the agencies to clarify that the guidelines only apply to consumers and customers as those terms are defined by The Gramm-Leach-Bliley Act (GLBA). Subsection 501(b) of the GLB Act requires that "each agency or authority... shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—(1) to insure the security and confidentiality of customer records and 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" (emphasis added). In the final rules governing Privacy of Consumer Financial Information, published in the Federal Register on June 1st, the agencies defined "customer" to mean a "consumer who has a customer relationship with a bank." Further, a consumer is defined by those regulations as "an individual who obtains or has obtained a financial product or service from a bank that is to be used primarily for personal, family, or household purposes..." (emphasis added). Given that the agencies have correctly applied the privacy regulation required under Title V solely to "individual" customers, Nationwide believes that this guidance should similarly apply only to the records of such customers.

Board of Directors

The agencies invite comment regarding the appropriate frequency of reports to the board of directors. Nationwide does not believe there should be a requirement for defined periodic reporting to the board. Often, reporting certain non-material information to a management level below the board, such as a committee of the board or a representative(s) of senior management, is a more efficient reporting mechanism than reporting to the full board. Further, the Nationwide companies have complex structures, including multiple boards that each has oversight responsibility for different affiliates and subsidiaries. The unique nature of each business will dictate the types of information that should be reported to each board.

Accordingly, Nationwide believes that the board or a committee of the board should be responsible for providing initial approval of the institution's security policies. Following the initial approval, Nationwide believes that management discretion should govern the frequency of reporting. Under this standard, management would be expected to report material exceptions to its board or a committee of the board on an as needed basis.

In the event the agencies do not support this proposal and decide to impose a requirement for periodic reporting, Nationwide believes that annual reports to the board or a committee of the board are more than sufficient.

Standards for Safeguarding Customer Information

Section II outlines proposed objectives for an institution's information security program. Nationwide supports goal oriented definitions but we are concerned that the objectives proposed by the agencies would create unrealistic and unattainable standards for financial institutions. The proposed guidelines require that a "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." (emphasis added).

First, Nationwide is concerned that use of the word "shall" suggests that institutions must assure absolute security protection. Nationwide follows sounds and prudent information security practices, and has implemented significant technical and human measures to protect our corporate systems and networks. However, the proposed standard is likely impossible for any financial institution to meet. Additionally, use of the word "any" as a modifier to the words "anticipated threats," and "customers or risk" in subsections 2 and 3 is overly broad. Finally, Nationwide is confused by the use of the word "inconvenience" in this context. While we believe that minimizing customer inconvenience is hallmark of good customer service, the concept of inconvenience is not an appropriate standard for these security guidelines.

Title V of the GLB Act requires the regulators to "establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards..." (emphasis added). To address these concerns, Nationwide suggests the agencies adopt the following language:

Objectives. A financial institution's information security program shall be designed to reasonably: 1. Promote the security and confidentiality of customer information; 2. Protect against 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 to customers or risks to the safety and soundness of the institution."

Nationwide believes that use of the term "appropriate" in the GLB statute supports inclusion of the phrase "...be designed to reasonably..." in the final regulations.

The agencies indicate in the preamble to the proposed regulation that "[f]or purposes of the guidelines, unauthorized access to or use of customer information does not include access to or use of customer information with the customer's consent." Nationwide agrees with this standard. For example, the practice of "screen scraping,"— where a customer provides a third party with authorization to access the customer's financial information— often occurs without the knowledge of the financial institution. In such situations, financial institutions should not be held responsible because the customer has clearly authorized access to their account and associated information. Consistent with this view, Nationwide strongly encourages the agencies to include language within the text of the guidelines themselves that reflects the language referenced above that is already included within the preamble.

Manage and Control Risk

In III(C)(1)(d) the agencies also propose instructing institutions to "consider appropriate encryption of electronic customer information, including while in transit or in storage on networks or system to which unauthorized individuals may have access." This language would require encryption in many cases where encryption is not appropriate. Encryption can be a complex and sophisticated approach to protecting confidential data. Requiring institutions to use encryption when it is not necessary could impair two-way electronic communication between financial institutions and their customers. Nationwide recommends the agencies change this section to focus on protection of customer data rather than a particular methodology for doing so. For example, Nationwide suggests the following language to replace the proposed language:

III(C)(1)(d) "Procedures to protect the confidentiality of electronic customer information, for example by encryption of electronic customer information, including while in transit or in storage on networks or systems not controlled and monitored by the bank or its agents."

The agencies invite comment on the degree of detail that should be included in the Guidelines regarding a risk management program. Nationwide strongly encourages the agencies to adopt guidelines that provide institutions sufficient flexibility to adopt policies and procedures that best reflect appropriate business and risk management practices for each individual institution.

The agencies ask for comment on whether specific types of security tests, such as penetration tests or intrusion detections should be required. Nationwide opposes requiring specific types of tests. Rather, each institution should have the flexibility to design and implement a testing program that is appropriate for their particular systems and requirements. This approach will allow institutions to develop and implement testing programs that are appropriate given the sophistication of each system being tested. Nationwide believes that this is consistent with supervision-by-risk principles. Additionally, allowing institutions this appropriate flexibility will promote innovation and improvement that will lead to better security.

The agencies also invite comment regarding the appropriate degree of independence that should be specified in the guidelines in connection with the testing for information security systems and the review of test results. Nationwide supports the standard put forth in OCC Bulletin 98-38 on Technology Risk Management: PC Banking. The section entitled Audit/Quality Assurance includes the following standard:

"An objective review of PC banking systems should identify and quantify risk, and detect possible weaknesses in the bank's risk management system as it pertains to PC banking. Management may rely on internal audit, external audit, or other qualified professional sources to conduct this review…".

Nationwide supports this "objective review" standard. We should have the flexibility to develop an independence standard that reflects the institution's culture, management reporting structure, and business activities, as well as sound business practices. Developing a one-size-fits-all approach for review of each institution's security standards will not properly reflect the needs or demands of each individual system.

Consistent with this view, Nationwide encourages the agencies to strike from section III(C)(3) the words "Test shall be conducted, where appropriate, by independent third parties or staff independent of those that develop or maintain the security programs. Test results shall be reviewed by independent third parties or staff independent of those that conduct the test." It would be appropriate to insert in its place similar language to that cited above from OCC Bulletin 98-38.

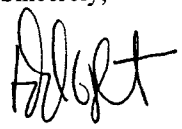
Outsourcing Arrangements

Nationwide believes that the proposed section governing oversight of outsourcing arrangements would create a standard that financial institutions will be unable to meet, particularly as it refers to "monitoring" of outsourcing agreements. For example, it would be nearly impossible for Nationwide to "monitor" compliance by mail houses and other third-party vendors. Rather, Nationwide supports a standard that requires initial due diligence that reflects each institution's business structure and complexity and ensures initial compliance by third parties with appropriate protection standards. Further, the guidance should explicitly recognize that the degree of sensitivity of the information to which the third party provider has access should be considered during the due diligence process. Each institution could be expected to include provisions in contracts to promote the protection of customer information.

CONCLUSIONS

Nationwide thanks the agencies for consideration of our comments. The agencies face a difficult and complex task in developing regulations in this area that do not place an undue burden on financial institutions. If can be of further assistance, please do not hesitate to contact me at 614-677-8651 or Nationwide's Chief Privacy Officer, Kirk Herath at 614-249-4420

Sincerely,



Edward G. Schwartz
Associate Vice President
Chief Information Security Officer
Nationwide