5 48,411

THE FINANCIAL SERVICES ROUNDTABLE

805 FIFTEENTH ST., N.W.
SUITE 600
WASHINGTON, D.C. 20005
TEL 202 289-4322
FAX 202 289-1903

E-MAIL: mail@fsround.org
WEBSITE: www.fsround.org

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
reg.comments@federalreserve.gov

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

Communications Division
Office of the Comptroller of the Currency
250 E Street, SW
Washington, D.C. 20219
Docket No. 00-13
reg.comments@occ.treas.gov

Manager, Dissemination Branch
Information Management & Services
Division
Office of Thrift Supervision
1700 G Street, NW
Washington, D.C. 20552
public.info@ots.treas.gov

Dear Sirs and Madams:

The Financial Services Roundtable and BITS appreciate 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. The Roundtable and BITS appreciate the work of the agencies in issuing the proposed rules and recognize 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.

The Financial Services Roundtable is a national association whose membership is reserved for 100 companies selected from the nation's 150 largest integrated financial services firms. The member companies of the Roundtable engage in a wide range of financial activities, including banking, securities, insurance, and other financial service activities. The mission of the Roundtable is to unify the leadership of large, integrated financial service companies in pursuit of three primary objectives:

- To be the premier forum in which leaders of the United States financial services industry determine and influence the most critical public policy issues that shape a vibrant, competitive marketplace and a growing national economy;
- To promote the interests of member companies in federal legislative, regulatory, and judicial forums; and
- To effectively communicate the benefits of competitive and integrated financial services to the American public.

The Roundtable is a CEO-driven association that advocates the interests of integrated financial institutions primarily in the Congress, the federal agencies, and federal courts.

BITS, the Technology Group for The Financial Services Roundtable, was created in 1996 to foster the growth and development of electronic commerce in an open environment for the benefit of financial institutions and their customers. BITS promotes safety and soundness in financial services and e-commerce. BITS is governed by a Board of Directors comprised of the Chairmen and CEOs of many of the largest U.S. financial services holding companies, as well as representatives of the American Bankers Association (ABA) and the Independent Community Bankers of America (ICBA). For more information, visit the BITS Web site at www.bitsinfo.org.

GENERAL COMMENTS

The Financial Services Roundtable and BITS support issuing the proposed guidance in the form of "Interagency Guidelines" rather than regulations. The practical effect of this decision is limited, since Roundtable members have every intention of, and will be responsible for, complying with the final standards regardless of the form in which they are issued. However, 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

The Roundtable and BITS agree that rescission of the Year 2000 Standards for Safety and Soundness is appropriate at this time.

Scope of Guidelines

The agencies invite comment on the scope of the guidelines. The Roundtable and BITS urge 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, the Roundtable and BITS believe 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. The Roundtable and BITS do 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, many Roundtable member companies have complex structures, including multiple boards that each have oversight responsibility for different affiliates and subsidiaries. The unique nature of each business will dictate the types of information that should be reported, the frequency of reporting required, and the management level at which the reporting should occur.

The references to board involvement should be replaced with a statement that information security is an integral part of each institution's Risk Management Program. As with other types of risk, the specific processes for managing risks to information security – including the nature, degree, and frequency of board involvement – should be left to the management and board of the institution to determine. Financial institutions must retain the discretion to design their information security programs in a manner appropriate to their size, organizational structure, business lines, and geographic dispersion.

Accordingly, the Roundtable and BITS believe that the board or a committee of the board should be responsible for providing initial review of the institution's security policies. Following the initial review, the Roundtable and BITS believe 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, the Roundtable and BITS believe 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. The Roundtable and BITS support goal-oriented definitions but 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, the Roundtable and BITS are concerned that use of the word "shall" suggests that institutions must assure absolute security protection. Our member companies, among the most advanced and sophisticated in the world, do an admirable job of protecting sensitive data. However, this standard is likely impossible for any institution to meet. Additionally, use of the word "any" as a modifier to the words "anticipated threats," and "customer or risk" in subsections 2 and 3 is overly broad. Finally, the Roundtable and BITS are confused by the use of the word "inconvenience" in this context. While the Roundtable and BITS believe that minimizing customer inconvenience is a 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, the Roundtable and BITS suggest the agencies adopt the following language: Objectives. A bank'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 bank." The Roundtable and BITS believe 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." The Roundtable and BITS agree 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 since the customer has clearly authorized access to his or her account and associated information. Consistent with this view, the Roundtable and BITS strongly encourage the agencies to include language within the text of the guidelines that reflects the language referenced above that is already included within the preamble.

Manage and Control Risk

The agencies list proposed factors that an institution should consider when evaluating its security policies. One of these, listed as factor III(C)(1)(a), applies to "access rights to customer information."

The Roundtable and BITS believe that this is intended to ensure that financial institutions have appropriate security measures in place to prevent unauthorized access to customer information.
However, this statement could be misinterpreted to apply to a customer's right to access financial information maintained by a financial institution under laws such as the Fair Credit Reporting Act. Accordingly, The Roundtable and BITS encourage the agencies to delete this factor. If the agencies intend to use this factor to promote appropriate standards against unauthorized access to customer's information, the Roundtable and BITS believe that the other factors listed, including III(C)(1)(b) and (c) appropriately address this area. At the least, the agencies should clarify that factor III(C)(1)(a) is not intended to create a new customer right to access financial information.

Additionally, the Roundtable and BITS note that the references to "companies" in factor III(C)(1)(b) should be struck. As stated previously in this letter, the Roundtable and BITS believe that these standards should only apply to consumers and customers as those terms are defined by GLBA. Accordingly, imposing standards for protection of "company" information should be outside the scope of this guidance.

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 systems 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. The Roundtable and BITS recommend the agencies change this section to focus on protection of customer data rather than a particular methodology for doing so. For example, the Roundtable and BITS suggest the following language to replace the proposed language:

> III(C)(1)(d) "Procedures to protect the confidentiality of electronic customer information, for example, but not limited to, 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. The Roundtable and BITS strongly encourage 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. The Roundtable and BITS oppose 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. The Roundtable and BITS believe 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. The Roundtable and BITS support 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...".

The Roundtable and BITS support this "objective review" standard. Each institution should have the flexibility to develop an independent 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 serve the needs or demands of each individual system.

Consistent with this view, the Roundtable and BITS encourage the agencies to strike from section III(C)(3) the words, "Tests 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

The Roundtable and BITS believe 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 financial institutions to "monitor" compliance by mail houses and other third-party vendors. Any obligation to audit, monitor, or inspect would be extremely burdensome to financial institutions and their service providers, would be regarded as highly intrusive by service providers (especially those with large numbers of clients), and

would significantly increase costs to the institutions and their customers. Rather, the Roundtable and BITS support 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.

BITS has formed a working group to evaluate the control, security, privacy and customer confidentiality issues associated with outsourced relationships. This working group will evaluate the risks, benefits and control requirements from the Request for Proposal (RFP) stage through the audit and assessment process. The group will review current risk assessment practices, as well as opportunities to develop new ones, such as the development of outsourcing criteria by the BITS Financial Services Security Laboratory. The work product of this group will help shape industry requirements.

CONCLUSIONS

The Roundtable and BITS thank 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 the Roundtable and BITS or any of our member companies can be of further assistance, please do not hesitate to contact me, Roundtable President Steve Bartlett or BITS CEO Catherine A. Allen at (202) 289-4322.

Sincerely,

Richard M. Whiting

Richard M. Whiting
Executive Director and
General Counsel