15

citigroup

CITIGROUP
BANK REGULATORY OFFICE
JEFFREY A. WATIKER
425 PARK AVENUE
2ND FLOOR/ZONE 2
NEW YORK, NY 10043
PHONE: (212) 559-1864
FAX: (212) 793-4403
EMAIL: jeffrey.watiker@citicorp.com

FAX TRANSMISSION
Total # of pages including this page: 9

DATE: 08/25/00

TO:	FAX:	TEL:
Communications Division, OCC	202 874-5274	
Mr. Robert E. Feldman, FDIC	202 898-3838	
Ms. Jennifer J. Johnson, Fed	202 452-3819	
Manager, Dissemination Branch Information Management & Services Division, OTS	202 906-7755	

2000 AUG 28 A 8:28

RE: Comment Letter on Proposed Interagency Guidelines on Safeguarding Customer Information

COMMENTS:

HARD COPY WILL FOLLOW.

Attachment

Carl V. Howard
General Counsel
Bank Regulatory

Citigroup Inc.
425 Park Avenue
2nd Floor/Zone 2
New York, NY 10043

Tel 212 559 2938
Fax 212 793 4403

15

August 25, 2000

Communications Division
Office of the Comptroller of the Currency
250 E Street, SW
Third Floor
Washington, DC 20219
Attn: Docket No. 00-13

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

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

Manager, Dissemination Branch
Information Management & Services
Division
Office of Thrift Supervision
1700 G Street, NW
Washington, DC 20552

Re: Joint Notice of Proposed Rule Making:
Interagency Guidelines Establishing Standards
For Safeguarding Customer Information.

Dear Sirs and Madams:

Citigroup is a financial services holding company with a variety of subsidiaries in the United States, including national banks, state non-member banks, and federal savings associations. This letter is in response to the joint request from 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") for comment on their proposed interagency guidelines ("Proposed Guidelines") establishing standards for safeguarding customer information (the "Joint Notice"). 65 Fed. Reg. 39472 (2000).[1]

When finalized, the Proposed Guidelines will implement Sections 501 and 505(b) of the Gramm-Leach-Bliley Act (the "GLBA"). Section 501 requires the Agencies to establish "appropriate" standards for the financial institutions subject to their respective jurisdictions relating to administrative, technical and physical safeguards for customer records and information. Section 505(b) directs the Agencies to implement these standards in the same manner, to the extent practicable, as the standards that the Agencies have prescribed pursuant

[1] The Joint Notice also includes a proposal to rescind the Agencies' Year 2000 standards for safety and soundness. Citigroup agrees that the Agencies should rescind those Year 2000 standards.

to Section 39(a) of the Federal Deposit Insurance Act (the "FDIA"). The Agencies have implemented the Section 39(a) standards (which apply to banks and thrifts, but not to holding companies) through uniform guidelines, rather than regulations. 60 Fed. Reg. 35674 (1995).

Citigroup places high importance on safeguarding customer records and information and, in general, we support the Proposed Guidelines both as to content and as to tone. We do, however, offer below several suggestions that would improve the Proposed Guidelines either by making them more effective at safeguarding customer information and records, or by making them less burdensome on financial institutions, or both.

In reviewing the Proposed Guidelines we have been guided by the following principles:

1. The Guidelines should be as consistent as possible with the Section 39(a) standards and with the Agencies' recently adopted privacy rules implementing Title V of the GLBA (the "Privacy Rules").

2. Although the Guidelines apply to individual banks, thrifts and holding companies (hereinafter "Covered Institutions") many Covered Institutions are part of multi-company banking organizations and the Guidelines should be designed to accommodate the types of customer information security programs that work best for multi-company organizations.

3. The Guidelines should provide Covered Institutions and multi-company banking organizations with sufficient flexibility to adopt policies and procedures that best reflect appropriate business and risk management practices for their institutions or organizations. Accordingly, although the Guidelines should require Covered Institutions to (i) assess customer information security risks, (ii) develop security programs to address those risks and (iii) test and evaluate their security systems, the Guidelines should not be overly specific in dictating how Covered Institutions accomplish these tasks. Over specification runs a serious risk of undermining security both because (i) Covered Institutions could be forced to deploy their resources inefficiently and/or ineffectively and (ii) the Guidelines could stifle innovation and self-improvement.

4. Consistent with Congress' mandate that the Agencies establish "appropriate" standards, the standards should strike a reasonable balance between affording protection for customers records and information and not imposing undue costs and burdens on Covered Institutions. Accordingly, the Agencies should avoid guidelines that might require Covered Organizations to design programs that are unreasonably burdensome or expensive.

Our specific recommendations are as follows:

A. Guidelines are Preferable to Rules or Regulations.

Citigroup supports issuing the proposed standards as guidelines, rather than regulations. Guidelines will provide a greater degree of flexibility to Covered Institutions without imposing any additional risks to the safety of customer information or compromising safety and soundness. Moreover, because the Section 39(a) standards were issued as guidelines, implementation of these standards as guidelines is consistent with Congress' mandate in Section 505(b) of the GLBA that the Agencies implement the standards for safeguarding customer information in the same manner, to the extent practical, as the Section 39(a) standards.

B. Scope of the Guidelines -- Definition of "Customer."

The Agencies should clarify that the Guidelines apply only to the records and information of individual retail customers. Subsection 501(b)(1) of the GLBA directs the Agencies to adopt standards to protect "customer records and information." In construing this language, we believe that the Agencies should act consistent with the Privacy Rules. The Privacy Rules define "customer" to mean a "consumer who has a customer relationship with a bank." The Privacy Rules further define a "consumer" as "an individual who obtains or has obtained a financial product or service from a bank to be used primarily for personal, family or household purposes ...". Consistent with these Rules, the Guidelines should apply only to records and information of individual consumers who have a retail customer relationship with a Covered Institution.

C. Standard for Safeguarding Customer Information.

The "Objectives" set forth in item II.B of the Proposed Guidelines should be rewritten to rely less on importing statutory language from Section 501(b) of the GLBA. Instead, the Agencies should craft language that captures Congress' intent without using words that set unachievable or overly broad objectives. For example, although Section 501(b) uses the word "insure," the Agencies should exercise discretion and not import that word into item II.B because this might cause Covered Institutions to believe that they were expected to design a system with a one hundred percent guarantee for protecting customer information. We do not believe that this was Congress' intent, as this could, in the case of many Covered Institutions, lead to an irrational allocation of resources.

Similarly, the Agencies should not import the word "any" from Section 501(b) as a modifier to the words "anticipated threats or hazards" and "customer," because the word "any" makes the objectives overly broad. Finally, the words "be designed to reasonably" should be added

after the word "shall" because use of the word "shall" suggests that Covered Institutions must ensure absolute security protection, a standard that would be unduly burdensome.

Again, the purpose for these changes is not to alter or dilute what Congress wanted to achieve. Rather, it is solely to craft a language that will make the Guidelines workable. Although we believe that the Agencies' authority to make word changes of this type is inherent in their rulemaking authority, it is especially apt in this case where Section 501 of the GLBA expressly directs the Agencies to adopt "appropriate" standards. If the use of the word "appropriate" is to have meaning, it surely means, at a minimum, that the Agencies are empowered to make the types of changes we suggest.

If the Agencies adopt each of these recommendations, item II.B. would read as follows:

> 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 or inconvenience to customers or risk to the safety and soundness of the bank.[2]

If the Agencies decide not to accept our proposed changes to item II.B, then, at a minimum, we request the Agencies state expressly, either in the Guidelines or in preamble language, that the Agencies do not expect that financial institutions would be able to provide a one hundred percent guarantee for protecting customer information.

D. Access with Customer Consent.

Citigroup supports the statement in the preamble of the Joint Notice 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." 65 Fed. Reg. at 39475. Covered Institutions should not be held responsible for disclosing data to the customer or to a third party where there is a customer consent or a customer's direction to do so. Accordingly, we recommend that the Agencies include this preamble language in the text of the Guidelines themselves.

[2] Although we intend our comments to apply with equal force to each of the Agencies, where we offer proposed language we, for simplicity's sake, will always use the term "bank," even though a different term might be more appropriate in contexts where the Covered Institution is a thrift or a bank holding company.

E. Corporate Information Security Officer.

Although (i) we endorse the use of one or more corporate information security officer(s) who has lead responsibility for information security and (ii) we believe that it can be effective for multi-company banking organizations to centralize their information security oversight in one or more such persons, we do not believe that the Guidelines should require boards of directors to designate a corporate information security officer. This level of detail is best left to the discretion of each Covered Institution (or multi-company banking organization) which can adopt policies and procedures that best reflect its particular circumstances.

F. Assessment of Risk and Management and Control of Risk.

1. Financial Risk and Reputation Risk.

Item III.B (Assess Risk) and item III.C (Manage and Control Risk) should each be amended to clarify that Covered Institutions should take into account financial and reputation risk. Specifically, we recommend that:

(1) the second sentence in item III.B.1. be revised to read: "As part of the risk assessment, a bank shall determine the sensitivity of customer information, the degree of exposure and impact of loss to the institution (including financial risk and reputation risk), and the internal or external threats to the bank's customer information systems." (emphasis added); and

(2) the second sentence in item III.C.1. be revised to read: "Policies and procedures shall be commensurate with the sensitivity of the information, and the degree of exposure and impact of loss to the institution, as well as the complexity and scope of the bank and its activities." (emphasis added).

2. "Access Rights" to Customer Information.

Item III.C.1.a. lists "access rights to customer information" as a factor that a Covered Institution should consider when evaluating its security policies. Although this item was probably intended to ensure that Covered Institutions have appropriate security measures in place to prevent unauthorized employee or third party access to customer information and records, we are concerned that the item could be misinterpreted to apply to a customer's right to access certain financial information maintained by a Covered Institution under laws such as the Fair Credit Reporting Act. To avoid this confusion (and because preventing unauthorized access is already appropriately addressed by items III.C.1.b. and III. C.1.c.), we recommend that the Agencies delete item III.C.1.a. If the Agencies do not agree with our

suggestion to delete item III.C.1.a., then, at a minimum, they should state in the Guidelines or in preamble language that item III.c.1.a. is not intended to create a new customer right to access financial information.

3. Encryption.

As proposed in the Joint Notice, item III.C.1.d. would require encryption for all customer data in storage (regardless of the level of protection surrounding that storage) on networks and systems that are controlled by the Covered Institution. Because such a requirement would not meaningfully increase the security of customer information and would be unduly burdensome to implement, we recommend that item III.C.1.d. be amended to read:

> "Procedures to protect the confidentiality of electronic customer information, such as 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."

4. Dual Control Procedures, Segregation Of Duties And Employee Background Checks.

We believe that item III.C.1.f. should not emphasize whether a Covered Institution specifically utilizes dual control procedures, segregation of duties and/or employee background checks, but rather whether the institution has appropriately considered procedures to protect against the types of mistakes and misconduct for which these procedures afford protection. Accordingly, we recommend that item III.C.1.f. be revised to read:

> "Procedures to protect against mistakes and misconduct, such as, for example, dual control procedures, segregation of duties, and/or employee background checks for employees with responsibility for or access to customer information."

5. Intrusion Detection.

a. Clarification/Amendments of Item III.C.1.h.

We recommend that item III.C.1.h. (which, as proposed by the Agencies, would require Covered Institutions to consider appropriate "[m]onitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems") be modified to make it more consistent with the treatment of "computer intrusion" in the Suspicious Activity Report ("SAR") forms. The SAR form (as revised in June 2000) contains a check box for "computer intrusions." For purposes of this check box, the SAR form defines the act of computer intrusion in a way that expressly excludes attempted intrusions of websites or other non-critical information systems of the institution that provide

no access to institution or customer financial or other critical information. We recommend that item III.C.1.h. be amended to include this exclusion. We also recommend that the Agencies follow the SAR approach and include no specific requirement to "monitor" systems.

Even if the Agencies do not make these changes, at a minimum, item III.C.1.h. should be amended by adding (at the end) the words "at public entry points." Without this change, the item might be read to require intrusion detection at nonpublic entry points which would, in our view, impose substantial costs on Covered Institutions without a commensurate benefit to the customers.

b. Discretion to Design and Implement Security Tests.

The Agencies also request comment on whether specific types of security tests, such as penetration tests or intrusion detection tests, should be required. We believe that the decisions concerning testing programs, including the types of test, should be left to the discretion of each Covered Institution. Each institution should have the flexibility to design and implement a testing program that is appropriate for their particular systems and requirements. Such an approach is consistent with supervision-by-risk principles and would promote innovation and self-improvement that should, in the long run, lead to better security.

G. Staff Training.

In order to ensure that the Guidelines give Covered Institutions necessary flexibility in the design and implementation of their staff training programs, item III.C.2 should be amended to add the words "as appropriate" after the words "Train staff."

H. Testing Systems and Review of Test Results.

The Agencies invite 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. We recommend that the Agencies permit institutions to follow an "objective review" standard akin to 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 weakness 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..."

Adoption of this "objective review" standard would afford institutions the appropriate flexibility to develop testing standards and appropriate ways of reviewing test results that reflects particular risks that apply to that institution.

Consistent with adoption of this flexible standard, we recommend that item III.C.3 be amended by deleting its last two sentences (which, by their terms, require (i) tests to be conducted, "where appropriate" by persons independent of those that develop or maintain the security programs and (ii) test results to be reviewed by parties independent of those that conducted the test). In our view, the requirements in these sentences are overly restrictive and would, in many instances, impose undue costs and undue complexity to the testing process. In place of these sentences, the Agencies should insert language similar to that cited above from OCC Bulletin 98-38.

*****

Citigroup appreciates this opportunity to comment on the Joint Notice. If you have any further questions or if we can provide any additional information, do not hesitate to call me at 212/559-2938 or my colleague, Jeffrey Watiker, at 212/559-1864.

Very truly yours,

Carl Howard

Carl V. Howard
General Counsel—Bank Regulatory

cc: Viola Spain
Jeffrey Watiker