



August 24, 2000

VIA FEDERAL EXPRESS

Office of the Comptroller  
of the Currency  
Communications Division  
250 E Street, S.W.  
Washington, D.C. 20219  
Attention: Docket No. 00-13

Robert E. Feldman  
Executive Secretary  
Federal Deposit Insurance  
Corporation  
550 17<sup>th</sup> Street, N.W.  
Washington, D.C. 20429  
Attention: Comments/OES

2000 AUG 25 P 2:49  
DISSEMINATION BRANCH  
OFFICE OF THRIFT SUPERVISION

Jennifer J. Johnson  
Secretary  
Board of Governors of the  
Federal Reserve System  
20<sup>th</sup> and C Streets, N.W.  
Washington, D.C. 20551  
Attention: Docket No. R-1073

Manager, Dissemination Branch  
Information Management & Services  
Division  
Office of Thrift Supervision  
1700 G. Street, NW  
Washington, DC 20552  
Docket No. 2000-15

Re: Proposed Interagency Guidelines Establishing Standards for Safeguarding  
Customer Information

Dear Ladies and Gentlemen:

BANK ONE CORPORATION is writing to comment on the proposed Interagency Guidelines Establishing Standards for Safeguarding Customer Information (the "Guidelines") issued jointly by the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision (together, the "Agencies") under the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) (the "GLB Act").

BANK ONE CORPORATION ("BANK ONE") is a multi-bank holding company headquartered in Chicago, Illinois, with offices located in Arizona, Colorado, Delaware, Illinois, Indiana, Florida, Kentucky, Louisiana, Michigan, Ohio, Oklahoma, Texas, Utah, West Virginia and Wisconsin. BANK ONE also operates numerous non-bank subsidiaries that engage in credit card and merchant processing, consumer finance, mortgage banking, insurance, trust and investment management, brokerage, investment and merchant banking, venture capital, equipment leasing and

data processing. First USA Bank, N.A., the largest VISA issuer in the United States, is a subsidiary of BANK ONE.

BANK ONE appreciates the opportunity to comment on the Proposed Guidelines released simultaneously by your Agencies. We are eager to work with the Agencies to develop workable Guidelines that addresses the concerns of both banks and consumers, and allow the development of new products and technology within the banking industry. We place a high priority on addressing the information security concerns of our customers to insure their continued confidence in our institution and the financial services industry. We thank the Agencies for allowing us to take part in the development of these Proposed Guidelines.

## **I. Introduction**

### **C. Definitions**

The Agencies have asked for comments on the scope of the Guidelines. We strongly urge the Agencies to clarify that the Guidelines apply only to consumer customer information, and not to information about business customers. To apply the Guidelines to business customer information would expand the coverage of the GLB Act beyond what was intended by Congress. The GLB Act extends certain protections to “consumers”, and a consumer is defined in Section 509(9) of the GLB Act as “an individual who obtains, from a bank, financial products or services which are to be used primarily for personal, family or household purposes”. There is no indication in the GLB Act or the legislative history that Congress intended to extend the protections of the GLB Act to corporations or other business entities. Limiting the scope of the Guidelines to the records of consumer customers is consistent with the plain language of the GLB Act.

## **II. Standards for Safeguarding Customer Information**

### **B. Objectives**

Bank One is concerned that the objectives proposed by the Agencies in subsection B. would create unrealistic and unattainable standards for banks. The proposed Guidelines require that:

“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.”

We are concerned this language requires that institutions must insure absolute security protection. While we believe that we do an excellent job of safeguarding customer data, it is virtually impossible for any bank to meet this absolute standard. Additionally, the requirement to protect against “any anticipated threats or hazards” is overly broad. We also suggest that the reference to “inconvenience to any customer” is inappropriate in this context. While we believe that minimizing customer inconvenience is a hallmark of good customer service, the concept of inconvenience is

outside of the scope of the GLB Act and should be outside of the scope and purpose of the Guidelines.

To address these concerns, we suggest the following language:

“B. Objectives. A bank’s information security program shall be designed to: (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.”

### **III. Development and Implementation of Information Security Program**

#### **A. Involve the Board of Directors and Management**

The Agencies invited comment regarding the appropriate frequency of reports by bank management to its board of directors about the information security program. While we agree that it is appropriate for a bank’s board of directors to be involved in developing and monitoring a bank’s information security program, we believe that the Guidelines should provide a bank with the flexibility to determine the proper level and frequency of the board’s involvement. We do not believe it is necessary for the Guidelines to specify a reporting interval in which the bank’s management team must report to the board. We believe that, following the initial approval, 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 requirement and decide to impose a requirement for periodic reporting, we believe that annual reports to the board or a committee of the board are more than sufficient.

In addition, the Guidelines should provide a bank’s board with the flexibility to determine how best to carry out its duty to be involved in the development of the bank’s information security program. For example, the Guidelines should clarify that a bank’s board of directors may delegate to a committee of the board primary responsibility for involvement in the bank’s security programs, rather than have the entire board actively involved throughout the process.

#### **C. Manage and Control Risk**

*Access Rights to Customer Information.* Section III.C.1.a. of the proposed Guidelines state that, in establishing its policies and procedures, a bank should consider appropriate “access rights to customer information”. We believe that this language is ambiguous and should be clarified or deleted. Customers currently have access to bank records through periodic account statements and credit reports. We believe that further access requirements would extend beyond the language of the GLB Act. Section 501 of the GLB Act does not create any independent substantive right of customers to have additional access to information that relates to them, nor do the final Privacy Regulations impose additional access requirements.

To the extent that the reference to “access rights” is not intended to address access rights for customers, but instead is intended to suggest that a bank should consider placing access controls on customer information systems, such as restricting access to customer information to properly authorized employees, the Agencies should revise this reference in the Guidelines to make this clear.

*Encryption.* The Agencies should make it clear in the Guidelines that a bank is not required to encrypt customer information each time the data is transmitted to a service provider or other third party. Encryption procedures are expensive for banks to implement and may be unwarranted depending on, among other things, the sensitivity of the type of data transmitted and the degree of risk that unauthorized individuals may have access to the data. Under the Guidelines, a bank should be provided the flexibility to decide when it is appropriate to use encryption technology.

In subsection III.C.1.d., the Agencies also propose that banks should 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 requirement appears to 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 banks and their customers. We recommend that the Agencies change this section to focus on protection of customer data rather than a particular methodology for doing so. Therefore, we suggest the following language to replace the proposed language in subsection III.C.1.d:

“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.”

*Independent Third Party Testing (Subsection III.C.3.).* The Guidelines should not require that the tests or review of tests be conducted by persons who are not employees of the bank. Requiring a bank to hire outside consultants to perform tests or review test results would impose unnecessary costs on banks with no benefit to consumers. A bank should have the flexibility to use its own internal resources, such as its internal audit division, to perform tests and review test results.

In addition, banks should have flexibility under the Guidelines to decide how best to ensure that: (1) the employees that are conducting the testing are independent of those employees that are developing or maintaining the security programs; and (2) the employees that are reviewing the test results are independent of those employees that are conducting the tests. The Agencies should not set forth specific measures that a bank must follow when it uses its employees to conduct testing and review test results.

#### D. Oversee Outsourcing Arrangements.

The proposed Guidelines state that a bank must 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 the Guidelines.

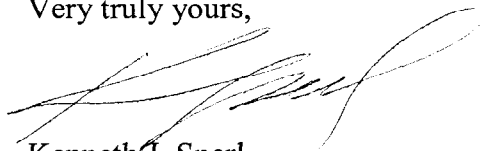
The Agencies should make it clear in the Guidelines that banks are not required to affirmatively audit the activities of its service providers to ensure that they have implemented an effective information security program. Instead, it should be sufficient for a bank to contractually require its service providers to implement information security programs and then to enforce those contractual provisions should the bank become aware of evidence of a breach of those contractual provisions. A bank realistically cannot be expected to audit each service provider to ensure that such parties are complying with the Guidelines, but should instead be expected to enforce contractual obligations should violations occur.

Further, the Agencies in the Guidelines should not set forth specific contract provisions that banks would be required to include in their contracts with service providers in connection with the security of information. A bank should have the flexibility to determine how best to craft its contract provisions with its service providers to ensure that the service providers are adequately ensuring the security of customer information.

If banks will be required to review all existing service provider contracts to insure that the contractual provisions are sufficient in light of the Guidelines, we strongly urge that banks be given additional time to complete this task. We suggest a provision like that contained in Section \_\_.18(c) of the Privacy Regulations, which gives banks a two-year period to amend existing joint marketing agreements to add the language required under Section \_\_.13 of the Privacy Regulation. Banks should be allowed a similar two-year period to review vendor contracts that do not fall under \_\_.13 of the Regulation, but may need to be amended because of the Guidelines.

Thank you for the opportunity to comment on these proposed Guidelines. If you have any questions concerning these comments, please contact Julie Johnson, Director of Information Policy and Privacy at (614)248-5654, or Andrea Beggs, Law Department, at (312) 732-5345.

Very truly yours,



Kenneth J. Sperl  
Deputy General Counsel  
Law Department