4/8/31.pdf

(24)

August 25, 2000

Attn: Docket No. R-1073
Ms. Jennifer J. Johnson, Secretary
Board of Governors of the Federal Reserve System
20th and C Streets, N.W.
Washington, DC 20551
E-mail: regs.comments@federalreserve.gov

Attn: Docket No. 00-13
Communications Division
Office of the Comptroller of the Currency
250 E Street, S.W., Third Floor
Washington, DC 20219
E-mail: regs.comments@occ.treas.gov

Attn: Comments/OES
Mr. Robert E. Feldman, Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street, N.W.
Washington, DC 20429
E-mail: comments@fdic.gov

Manager, Dissemination Branch
Information Management & Services Division
Office of Thrift Supervision
1700 G Street, N.W.
Washington, DC 20552
E-mail: public.info@ots.treas.gov

Subject: Joint Notice of Proposed Rule Making, Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness. FRB Docket No. R-1073, OCC Docket No. 00-13, OTS Docket No. 2000-15 and FDIC: RIN 3064-AC39.

FleetBoston Financial Corporation appreciates the opportunity to comment on the proposed rule making regarding the standards for safeguarding customer information

issued by the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision (collectively, the "Agencies"). FleetBoston Financial Corporation (hereinafter "Fleet") is the eighth largest financial holding company in the United States. An $185 billion diversified financial services company, it offers a comprehensive array of innovative financial solutions to 20 million customers in more than 20 countries and territories. Among the company's key lines of business are retail banking, with over 1,250 branches and over 3,400 ATMs in the Northeast; commercial banking, including capital markets/investment banking and commercial finance; investment services, including discount brokerage; and full-service banking through more than 250 offices in Latin America. Fleet is headquartered in Boston and listed on the New York Stock Exchange (NYSE: FBF) and the Boston Stock Exchange (BSE: FBF).

The safeguarding of customer information is something Fleet takes very seriously. Accordingly, we are pleased to offer the following comments.

General Comments

The proposed standards promulgated by the Agencies appear to be consistent with many of Fleet's existing policies and procedures with respect to safeguarding customer information. However, there are several sections within the guidelines which we would like further clarification.

In addition, while Fleet intends to comply with any standard issued by the Agencies, regardless of form, Fleet believes that the proposed standards for safeguarding customer information should be promulgated as interagency guidelines, and not in the form of regulations. By issuing these standards as guidelines, Fleet will not only be able to continue to enforce existing policies and procedures, but we will also have the flexibility to develop and institute new security policies and procedures to protect customer information as technology and technological capabilities evolve.

Rescission of Year 2000 Standards

Fleet believes that rescission of these standards is appropriate at this time.

Development and Implementation of Information Security Program

Board of Directors

As a large financial institution, Fleet has a number of current systems in place to oversee and approve information security policies. Fleet believes that its current reporting system, which includes periodic reports to the Audit Committee of the Board of Directors, is not only an effective means of reporting, but also ensures that only relevant and material information is communicated to the board. Accordingly, Fleet requests that it be able to retain its discretion as to the manner and frequency of reports to its Board of Directors.

Encryption of Electronic Customer Information

The proposed standard could mean that potentially all electronic transmissions of customer information would have to be encrypted in situations where encryption may not be the most suitable or appropriate method. To require encryption in every instance in which customer information is transmitted electronically may not only be unnecessary, but might hamper the relationship between Fleet and its customers by making electronic communication more complicated.

Fleet believes that the OCC's October 1999 Comptroller's Handbook on Internet Banking may also be of some guidance with regard to the issue of encryption of customer information. In relevant part, the Comptroller states that, " Internet banking systems should employ a level of encryption that is appropriate to the level or risk present in the systems. OCC is aware that stronger levels of encryption may slow or degrade performance and, accordingly, management must balance security needs with performance and cost issues. Thus, a national bank should conduct a risk assessment in deciding upon its appropriate level of encryption. The OCC does not mandate a particular strength or type of encryption. Rather, it expects management to evaluate security risks, review the cost and benefit of different encryption systems, and decide on an appropriate level of encryption as a business decision."[1]

While Fleet understands that the Handbook is only one point of reference from which guidance can be sought, we believe that this passage succinctly defines the issues and the factors that need to be considered regarding encryption. We believe that this passage recognizes the need for discretion with regard to the use of encryption, and that this discretion should be reflected in any standard promulgated by the Agencies. Accordingly, Fleet requests that financial institutions be given discretion in making the determination as to what kinds of electronic transmissions require encryption.

---

[1] Comptroller of the Currency, *Internet Banking, Comptroller's Handbook*, October 1999, page 19.

In addition, Fleet requests clarification of the terms "in transit" and "unauthorized individuals". ["I]n transit", as discussed above, could be construed to mean that encryption of customer information should take place with regard to internal transmissions of information between departments or business lines. Therefore, we request that "in transit" refer to information that is transmitted via a web server connected to the Internet.

The term "unauthorized individuals" is not clearly defined by the proposed guidelines as drafted. For instance, are there some instances in which a bank employee or a service provider could be deemed an "unauthorized individual" under the guidelines?

Employee Background Checks

In part, due to differing corporate policies prior to the Fleet/BankBoston merger, only some employees have been subject to background checks in the past. As a result, some employees who have access to and are responsible for the handling of customer information may not have been subject to a background check at the time of hire. While we recognize that the section gives banks a measure of latitude by stating that banks "should consider" such a policy, Fleet still might have to initiate retroactive background checks on thousands of employees, which would create an undue burden on Fleet. We request that the Agencies reconsider the use of such a broad definition, and consider a more narrow construction that would specifically address which types of employees should be targeted by this paragraph.

Response Programs

While Fleet is currently developing a Computer Emergency Response program that addresses the issue of unauthorized access to customer information systems, and agrees that this is a vital component of any risk management system, we do not believe that we should devise a plan that is too detailed in nature. We believe it would be more practical to devise a program that focuses on an overall plan structure with identified roles and responsibilities rather than cover specific responses for each and every situation that could occur. To attempt to identify every potential scheme and the corollary response would be a colossal task and the list would be obsolete prior to its' completion.

Testing of Controls in the Information Security Plan

Fleet believes that a "check and balance" system is appropriate to ensure that our systems are sound. However, we request that banks be allowed to maintain flexibility to determine when and if such tests should be conducted.

Oversight of Outsourcing Arrangements

Fleet believes that the placement of a monitoring requirement would create a standard that might be impossible to meet. In addition, we request clarification as to what kinds of monitoring should actually take place and to what degree. Fleet currently has systems in place to perform initial due diligence checks for new service providers on the electronic systems that will process Fleet customer data. We make every effort to ensure that the contract with the service provider includes a "right to audit" clause.

We request that the "monitoring" component of the standard be reconsidered to reflect our current practices, which include initial due diligence checks.

Conclusion

Fleet appreciates the opportunity to comment on the proposed standards, and we thank the Agencies for consideration of our comments. If we can provide any additional information or be of further assistance, please do not hesitate to contact me at (617) 346-4658.

Sincerely,

Agnes Bundy Scanlan
Managing Director, Corporate Privacy