



**NATIONAL RETAIL FEDERATION**

November 1, 2000

Secretary  
Federal Trade Commission  
Room H-159  
600 Pennsylvania Avenue, N.W.  
Washington, DC 20580

**Re: Gramm-Leach-Bliley Act Privacy Safeguards Rule, 16 CFR Part 313 --  
Comment**

Dear Mr. Secretary:

The **National Retail Federation** (“NRF”) submits these comments in response to the Federal Trade Commission’s (“FTC”) advance notice of a proposed rulemaking, 65 Fed. Reg. 54,186 (Sept. 7, 2000), concerning the development of the administrative, technical, and physical information “Safeguards Rule” required by § 501(b) of the Gramm-Leach-Bliley Act (“GLBA”), Pub. L. No. 106-102.

The National Retail Federation is the world's largest retail trade association with membership that comprises all retail formats and channels of distribution including department, specialty, discount, catalog, Internet and independent stores. NRF members represent an industry that encompasses more than 1.4 million U.S. retail establishments, employs more than 20 million people -- about 1 in 5 American workers -- and registered 1999 sales of \$3 trillion. NRF's international members operate stores in more than 50 nations. In its role as the retail industry's umbrella group, NRF also represents 32 national and 50 state associations in the U.S. as well as 36 international associations representing retailers abroad.

The following comments highlight those issues raised in the FTC's request for comments that are of particular concern to the NRF and its members.

Comments

- I. *The definition of “customer records and information” should be substantially similar to the definition of “nonpublic personal information.”*

The Safeguards Rule will implement § 501(b) of the GLBA. Section 501(b) requires the FTC and other agencies to establish standards that will, *inter alia*, “insure the security and confidentiality of customer records and information.”

We believe the Safeguards Rule definition of “customer records and information” should be substantially similar to the definition of “nonpublic personal information” under the FTC’s regulations concerning “Privacy of Consumer Financial Information” (“Privacy Regulations”), 16 C.F.R. § 313.3(n). The Privacy Regulations and the Safeguards Rule have the same focus – the protection of nonpublic personal information. The distinction between these regulations should lie in the risk addressed (*i.e.*, intentional disclosure in the case of the Privacy Regulations v. unintentional disclosure in the case of the Safeguard Rule), rather than the information protected.

GLBA and the Privacy Regulations define the information to be protected very broadly to include essentially any information obtained through, or in connection with offering or providing financial services or products. This broad definition was apparently felt sufficient to protect customers from intentional disclosure and it is counterintuitive that a broader category of information would need to be protected from unintentional disclosure. Such a distinction could lead to the illogical result of one set of GLBA regulations allowing the unrestricted intentional disclosure of customer information, while another requiring extensive security measures to protect the unintentional disclosure of that same information. Thus, we believe that the scope of records and information addressed by the Safeguards Rule should be congruent with and certainly no more extensive than the scope of the Privacy Regulations.

## II. *The Safeguards Rule should apply only to “consumers” who are “customers.”*

The Privacy Regulations define a consumer as “an individual who obtains or has obtained a financial product or service from [a financial institution] that is to be used primarily for personal, family, or household purposes, or that individual’s legal representative.” (16 C.F.R. § 313.3(e)(1)) The category of consumers includes the narrower category of “customers.” That narrower category is comprised of consumers with a “continuing relationship” with a financial institution. (16 C.F.R. § 313.3(h))

The Privacy Regulations reflect the fact that the GLBA imposes on financial institutions greater obligations with respect to customers than with respect to consumers. (*See*, 16 C.F.R. §§ 313.4-313.12 (imposing more stringent requirements with respect to customers than with respect to consumers)). Significantly, the GLBA requirements for “administrative, technical, and physical safeguards” refer only to customers. (GLBA § 501) Accordingly, we believe the Safeguards Rule should apply only to customers.

The FTC has specifically asked whether the Safeguards Rule should apply to both consumers and customers if a financial institution cannot separate consumer records and information from customer records and information. (*See* 65 Fed. Reg. 54,187 (Sept. 7 2000)) It is likely that, in some instances, a financial institution’s inability to segregate customer and consumer information will result in the application of the Safeguards Rule to consumers, as well

as customers. As discussed above, however, the GLBA discussion of safeguards refers only to customers, and that is the proper category to which the Safeguards Rule should be applied as a matter of legal obligation.

III. *Unauthorized access to customer information should not automatically trigger a customer notification requirement.*

We believe it would be unduly burdensome to require financial institutions to notify customers in every case of “unauthorized access” to customer information. (*See*, 65 Fed. Reg. 54,188 (Sept. 7, 2000)) If there is a requirement of customer notification in the event of unauthorized access, we believe such a requirement should be limited to those instances in which the unauthorized access results in some type of harm to the customer and the financial institution is aware that the customer has been harmed. Any broader requirement would be unworkable and could result in unduly alarming millions of customers when internal security procedures were not followed (*e.g.*, an unauthorized employee obtains access to a database for legitimate purposes by borrowing another’s password), with no harm to the customer. Unless and until unauthorized access leads to some measurable harm to a particular customer, providing notification would serve no purpose other than to upset the customer unnecessarily and perhaps induce the customer to take wholly unnecessary precautions like canceling credit cards that have not in fact been compromised.

IV. *The Safeguards Rule should not require financial institutions to grant customers periodic access to their records.*

The primary purpose of the Safeguards Rule is the security of customer information. As a general matter, there is an inverse relationship between the security of information and the extent of access to that information. Increased access generally results in less security, especially in an era when identifying the source of a request for access is not easy and fraudulent requests are predictable. We therefore believe the Safeguards Rule should not require periodic customer access, a requirement that would be in tension with the primary purpose of the Safeguards Rule. If access is important to serve other policy goals, it should be considered in a more relevant context.

V. *Boards of directors should not be required to be involved in information security programs.*

Pursuant to guidelines proposed 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 (“proposed Interagency Guidelines”), each financial institution would be required to involve its board of directors in information security policy. (*See*, 65 Fed. Reg. 39,471 (June 26, 2000)) Specifically, the proposed Interagency Guidelines state that “the board’s responsibilities are to: (1) [a]pprove the institution’s written information security policy and program that complies with these Guidelines; and (2) oversee efforts to

develop, implement, and maintain an effective information security program, including the regular review of management reports.” (*Id.* at 39,475)

We believe the Safeguards Rule should not emulate the proposed Interagency Guidelines with respect to the requirement of board of director involvement in information security policy. The information security environment changes extraordinarily rapidly and, therefore, information security policies must change rapidly as well. Given the large number of issues that must be overseen by many boards of directors, we believe it is impractical to require board of director involvement in something as complex and dynamic as information security policy.

This is especially true in an industry like retailing with firms large and small that employ highly diverse organizational structures. While a bank regulator might logically conclude certain functions should be placed in a bank’s board of directors to assure the safety and soundness of a federally insured depository institution, the firms subject to FTC jurisdiction take many different forms and compete in numerous businesses.

Information security is clearly an important matter, but it is no more important in terms of GLBA’s goals than a corporate privacy policy and the associated opt-out procedures. However, the Privacy Regulations do not mandate board involvement in the development and implementation of these policies and procedures. In fact, despite the enormously important issues addressed by other FTC regulations, we could find no similar requirement for board involvement in such matters. There is no compelling reason to break from this precedent in this instance.

The statutory goal of protecting customer information is not advanced by mandating board involvement and such a mandate would merely lead to inefficiencies in the development and implementation of the security program. Given the obligation to develop an information security program, the FTC overseeing community should be permitted to implement the program in accordance with its own policy implementation procedures.

VI. *In general, the Safeguards Rule should utilize flexible standards rather than imposing rigid rules and procedures.*

The previous comment is a specific manifestation of our general view that the Safeguards Rule should utilize flexible standards rather than imposing rigid rules and procedures. The enormous diversity in the FTC’s overseeing community, the wide range of protected customer information, and the pace of technological changes relevant to information security make rigid standards impractical.

GLBA-denominated financial institutions subject to the FTC’s broad Privacy Regulations are extraordinarily diverse – entities with significantly different financial resources engaging in a wide variety of business ventures. The Safeguards rule should be flexible enough to accommodate this diversity. A very specific procedural safeguard that is appropriate for one “financial institution” might be so resource-intensive for another that an attempt to implement it might preclude the effective implementation of other equally important safeguards.

In addition, the potential harm to the customer associated with the unauthorized access to customer information will vary greatly depending upon the sensitivity of the information. For example, the potential harm associated with the unauthorized access to a customer's credit card number is obviously greater than that associated with the unauthorized access to their name. Whereas both the credit card number and customer name must be protected from unauthorized access, additional security measures may be warranted to protect the former as a result of the relative sensitivity of that information. As this information may be maintained separately (*e.g.*, separate databases or fields within databases), the Safeguards Rule should allow the flexibility to fashion security measures that fit the relative sensitivity of the information.

Further, technology is moving so rapidly in this area that it would be impracticable for the regulations to mandate specific standards. Specific standards for security measures would need to be frequently modified to keep up with these changes but the rulemaking process is simply not nimble enough to keep pace with this changing technology.

In this regard, the proposed Interagency Guidelines provide a good model of the appropriate level of specificity and flexibility. The proposed Interagency Guidelines set forth a general process for development and implementation of a security program, and include various security measures to consider. However, in likely recognition of the futility of such an effort, the proposed Interagency Guidelines do not prescribe rigid security measures.

With regard to the question about whether the Safeguards Rule should "set forth minimum procedures a financial institution must follow, a minimum level of effectiveness financial institutions must maintain, or a combination of both," 65 Fed. Reg. 54,187 (Sept. 7, 2000), we believe it is generally preferable for the Safeguards Rule to establish a minimum level of effectiveness that financial institutions must maintain. It is the level of effectiveness that is ultimately important, and different institutions might need to utilize different procedures in order to maintain the same level of effectiveness.

### Conclusion

The NRF appreciates the FTC's consideration of these comments and commends the FTC's efforts with respect to developing the Safeguards Rule.

Sincerely,

Don Gilbert  
Senior Vice President, Information Technology

Mallory B. Duncan  
Vice President, General Counsel