



**NATIONAL RETAIL FEDERATION**



November 13, 2001

Secretary  
Federal Trade Commission  
Room 159  
600 Pennsylvania Avenue, N.W.  
Washington, D.C. 20580

Re: Comment on Standards for Safeguarding Customer Information, 16 CFR Part 314

Dear Mr. Secretary:

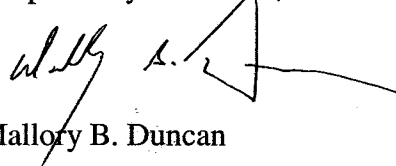
I believe the attached comments regarding Comment on Standards for Safeguarding Customer Information, 16 CFR Part 314, were filed by our office electronically the first of October.

Recently, while reviewing comments on the FTC website, we noticed that the National Retail Federation's ("NRF") comments were not included. Apparently, the e-mail was not received or did not go through. Accordingly, we are refileing them in paper format.

Because the NRF represents such a broad spectrum of companies who would be affected by the FTC's proposed standards; because the businesses we represent are those towards whom the Commission's proposed flexible standards appear to be directed; and, because our comments were timely filed, we ask that they be made a part of the official record in these proceedings and considered by the Commission in its deliberations.

If you have any questions, please feel free to contact me at 202-783-7971.

Respectfully submitted,



Malloy B. Duncan

MBD/elf  
Attachment

*The World's Largest Retail Trade Association*

Liberty Place, 325 7th Street NW, Suite 1100  
Washington, DC 20004  
202.783.7971 Fax: 202.737.2849  
www.nrf.com



**NATIONAL RETAIL FEDERATION**

October 1, 2001

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

Re: Comment on Standards for Safeguarding Customer Information, 16 CFR Part 314

Dear Mr. Secretary:

The National Retail Federation ("NRF") appreciates the opportunity to comment on the FTC's proposed rule regarding standards for safeguarding customer information, 66 Fed. Reg. 41162 (August 7, 2001).

NRF is the world's largest retail trade association, representing an industry that encompasses more than 1.4 million U.S. retail establishments and employs more than 20 million people – about 1 in 5 American workers – with registered sales of \$3.4 trillion annually. 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 United States. Many NRF members offer proprietary, private label or co-branded credit cards and/or engage in other activities which may bring them within the scope of Title V of the Gramm-Leach-Bliley Act (the "GLBA"), the FTC's privacy rule, and the proposed safeguards rule.

**General Comments**

The stated objectives of the proposed safeguards rule are (1) to ensure the security and confidentiality of customer records and information,<sup>1</sup> (2) to protect against anticipated threats or hazards to the security or integrity of such records, and (3) to protect against unauthorized access to, and use of, such records or information that could result in substantial harm or inconvenience to a customer. Proposed Section 314.3(b). In furtherance of these objectives, a financial institution would be required to implement a comprehensive written information security

---

<sup>1</sup> We note that the proposed rule uses the term "insure," rather than "ensure." We believe that the intent is to "ensure" the confidentiality of the customer information, and note that the FTC uses "ensure" in the Supplemental Information. 66 Fed. Reg., at 41164

*The World's Largest Retail Trade Association*

◆  
Liberty Place, 325 7th Street NW, Suite 1100  
Washington, DC 20004  
202.783.7971 Fax: 202.737.2849  
www.nrf.com

program that would contain the administrative, technical and physical safeguards that are appropriate to the size and complexity of the financial institution, the nature and scope of its activities, and the sensitivity of any customer information at issue. Proposed Section 314.3(a). The program must contain the elements set forth in Proposed Section 314.4 and must be reasonably designed to achieve the rule's objectives. *Id.* Thus, the proposed rule would give financial institutions the flexibility to design their own information safeguards programs as long as the program contained the rule's basic elements and met its stated objectives.

NRF supports the proposed rule's objectives and its aim of establishing clear, but flexible standards for financial institutions in safeguarding their customers' information. Our members rely on the security and integrity of their customer records in their business operations. Moreover, NRF members fully appreciate our customers' reasonable expectation that the nonpublic personal information they provide will be kept confidential and secure. For these reasons, many NRF members already have in place efficient and reliable procedures to safeguard the security and confidentiality of their customers' information. Moreover, the nation's million-plus retailers range in size and complexity of operation from large multinational corporations to sole proprietorships operating a single outlet. They comprise all retail formats and channels of distribution, including department, specialty, discount, catalog, Internet and independent stores. The vastly diverse structure and nature of NRF members and the industry demonstrate the need for the rule's requirements to be adaptable according to individual size, complexity and special circumstances.

For these reasons, NRF commends the FTC for proposing a "flexible" safeguard rule designed to allow businesses to adopt safeguards for customer information that are appropriate to each business, reflecting the nature of the products offered and the customer information handled. This flexibility should allow retailers with existing safeguard procedures to continue their existing practices with minimal modification and disruption.

While NRF thus supports the objectives of the safeguards proposal, we have some concerns as to its proposed scope, the "service provider" definition, aspects of the statement of objectives and required elements, and the proposed effective date with respect to existing service provider contracts. The following discussion explains the basis for these concerns.

### **Scope of Information Covered (Proposed Section 314.1(b))**

The proposed rule would apply to all "customer" information in a financial institution's possession, even if the information does not relate to the financial institution's own customers. *See* Proposed Section 314.1(b). Therefore, under the proposal, a financial institution would need to have special procedures to safeguard not only its *own* customer information, but that which it would receive from any other financial institution. Moreover, the FTC's Supplementary Information states that the proposal would impose direct obligations on *affiliates* of financial

institutions if they themselves are financial institutions and are in the possession of information that relates to the customers of their affiliated financial institution.

NRF believes the proposed coverage is unnecessary, unworkable and inconsistent with Congressional authority and intent. While all financial institutions should have in place procedures to safeguard nonpublic personal information received from nonaffiliated financial institutions, it does not follow that these financial institutions should have to adhere to the rule's specific, detailed requirements for safeguarding such information when it does not involve their own customers. The proposed rule ignores the fact that the FTC's Privacy Rule (16 CFR Part 313) already requires financial institutions to protect against unauthorized redisclosure of nonpublic personal information received from nonaffiliated financial institutions. 16 CFR §313.11. For that reason, financial institutions already have in place procedures to protect against the unauthorized disclosure of this information, and those procedures may well be different from those required under the safeguards rule for a financial institution's own customers. Imposing the proposed safeguards rule's specific requirements for non-customer information could require financial institutions to develop and implement new procedures for information that is already protected under the Privacy Rule. Establishing these new procedures would create unnecessary burdens, particularly on smaller businesses.

Not only is this broad coverage not necessary, it also appears to exceed Congressional authority and intent. The FTC's proposed safeguards rule is promulgated pursuant to GLBA subsection 501(b), which requires that the rule be established in "[i]n furtherance of the policy in subsection [501](a)." 15 U.S.C. §6801(b); GLBA §501(b). Subsection 501(a) requires financial institutions to safeguard their *own* customers' non public personal information:

It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of *its customers* and to protect the security and confidentiality of *those customers'* nonpublic personal information.

15 U.S.C. §6801(a); GLBA §501(a) (emphasis added).

Because the FTC's proposed rule would require financial institutions to adopt a safeguards program with respect to information they receive about *other* financial institutions' customers, the proposal is inconsistent with the express language of the GLBA and the Congressional intent that the safeguard standards for financial institutions apply to the institutions' *own* customers' nonpublic personal information.

In contrast to the FTC proposal, the security guidelines issued last January by the federal banking agencies implemented the Congressional policy with respect to scope. The banking agency guidelines stated: "the most reasonable interpretation of the applicable provisions of subtitle A of Title V of the Act is that a financial institution is obligated to protect the security

and confidentiality of the nonpublic personal information of *its* consumers *with whom it has a customer relationship*." Federal Banking Agency Guidelines/Joint Final Rule, 66 Fed. Reg. 8616 et seq., (emphasis added). Accordingly, the Office of the Comptroller of the Currency, the Federal Reserve System and the Federal Deposit Insurance Corporation guidelines define "customer" as "any *customer of the bank* as defined in [the Privacy Rule], *see id.* at 8633, 8635, 8638 (emphasis added), and the Office of Thrift Supervision's guidelines define "customer" as "any of *your customers* as defined in [the Privacy Rule]." *Id.* at 8640 (emphasis added). The FTC's rule should not exceed the scope of the banking agency guidelines.

Moreover, according to the Supplementary Information, financial institutions would be required "to ensure that customer information remains protected when it is shared with their *affiliates* and service providers," and "to ensure that the *affiliates* maintain appropriate safeguards for the customer information." 66 Fed. Reg., at 41164 (emphasis added). NRF can find no basis in the GLBA for any requirement that financial institutions enforce substantive provisions against *affiliates*. In fact, the rule itself does not impose any obligation on financial institutions to ensure anything with respect to affiliates, except to the extent that an affiliate would be a "service provider." (See proposed section 314.4(d), discussed below.) Finally, it is unclear by which means the FTC believes a financial institution could "ensure" appropriate safeguards by any of its affiliates, over which it may have no control. Thus, the Supplemental Information creates unnecessary ambiguity.

The FTC's final rule should make clear that it does not apply to affiliates of financial institutions unless they are also financial institutions, and even in that case, the rule's substantive requirements should apply only with respect to a financial institution's own customer information. The final rule should also make clear that it does not impose any obligation on a financial institution with respect to affiliates or other separate corporate entities.

### **Definitions (Proposed Section 314.2)**

The definition of "service provider" should exclude attorneys, accountants and similar professionals who already are under strong ethical obligations under state licensing laws to maintain the confidentiality of the covered information. Requiring NRF members to have special contracts with these service providers would impose unnecessary burdens without any countervailing benefits to consumers.

### **Standards and objectives (Proposed Section 314.3)**

The proposal states that any information safeguards shall be "reasonably designed" to achieve its objectives. NRF believes that, for clarification purposes, the stated objectives themselves should contain a "reasonableness" qualification because *absolute* achievement of the objectives, and information security in general, is not possible and, therefore, not required.

### **Required elements of an information security program (Proposed Section 314.4)**

Under the proposed rule, one of the elements of an information security program would be the designation of an "employee" to coordinate the program. Small financial institutions may wish to outsource the coordination, implementation and maintenance of its security program. While "an employee" should be responsible for the information security program, the final rule should make clear that some or all of the compliance procedures may be outsourced.

Section 314.4(d)(1) would require covered entities to "[o]versee service providers, by: (1) selecting and retaining service providers that are capable of maintaining appropriate safeguards for the customer information at issue . . . ." This provision could be interpreted to impose a strict liability standard on the financial institution if the service provider failed to maintain appropriate safeguards. We, therefore, recommend that this section provide that the financial institution oversee service providers by "retaining service providers *that you have reason to believe* are capable of maintaining appropriate safeguards. . . ."

### **Effective Date: Proposed Grandfathering of Existing Contracts (Proposed Section 314.5)**

The proposed rule would require implementation of an information security program not later than one year from the date on which a final rule is issued. Proposed Section 314.5. One of the required elements is that the financial institution oversee service providers by, among other things, requiring the service provider by contract to implement and maintain appropriate safeguards for the customer information at issue. Proposed Section 314.4(d)(2).

The FTC has sought comment on whether it should provide for a two-year transition period with respect to the rule's effective date to allow the continuation of existing contracts with service providers, even if these contracts would not fully satisfy the rule's requirements. NRF urges such a grandfathering provision for existing contracts.

As discussed above, retailers have their own interest in the integrity and security of their customers' information, and retailers appreciate their customers' expectation that this information will be kept confidential and secure. Retailers subject to the GLBA should already have in place effective information security programs, including procedures to assure the confidentiality and security of customer information given to their service providers. Moreover, the proposed rule would require retailers to select and *retain* service providers that are capable of maintaining appropriate safeguards. Proposed section 314.4(d)(1). Therefore, once the rule is effective, financial institutions would have to comply with the *substantive* requirement of retaining service providers that with appropriate safeguards procedures. The proposed grandfathering would apply only to the requirement that contracts contain *language* requiring the service provider to implement and maintain specific safeguards. Because existing service provider contracts may not contain that specific language, compliance within the one year implementation period could entail executing new contracts with all service providers for the sole purpose of adding the new

language. That would be create an unnecessary burden, which would fall particularly hard on small businesses. A provision grandfathering existing service provider contracts for two years would enable the specific safeguards language to be added when the contracts are amended or renewed in the normal course of business. Such a provision would alleviate the compliance burden without in any way compromising the substantive requirement that financial institutions retain service providers with appropriate safeguards procedures.

\*\*\*

NRF appreciates the opportunity to comment on the FTC's proposed safeguards rule. Please do not hesitate to call me at (202) 783-7971 if you have any questions on this comment letter or if we can otherwise be of further assistance in connection with the proposal.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Mallory B. Duncan", with a stylized flourish extending to the right.

Mallory B. Duncan

RECEIVED  
MAY 10 2011  
10:09 AM  
FEDERAL RESERVE BANK  
WASHINGTON, DC