Intuit

Legal Department
P.O. Box 7850
Mountain View, California 94039-7850

October 9, 2001

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

Copy to GLB501Rule@ftc.gov

Re: Gramm-Leach-Bliley Act Privacy Safeguards Rule, FTC 16 CFR Part 314 – Comment

Ladies and Gentlemen:

Intuit Inc. ("Intuit") is a financial software and services company, the maker of Quicken®, QuickBooks® and TurboTax®. Intuit has a variety of other financial divisions, subsidiaries and partners. Intuit has a major online presence through its 17 Web sites which include http://www.quicken.com, http://www.quickenloans.com, and http://www.turbotax.com. Intuit's 18 years' experience in handling and securing customer data as well as its large customer base, make the company especially qualified to address the issue of safeguarding customer information.

Intuit appreciates the opportunity to submit comments on development of the Federal Trade Commission's ("FTC") security safeguards rule ("FTC Safeguards Rule" or "Rule") under Section 501(b) of the Gramm-Leach-Bliley Act ("GLB Act"), as requested in its notice of proposed rulemaking and request for comment ("Proposed Rule"). Intuit appreciates the consideration given by the FTC to its previous comments (October 24, 2000) in response to the advance notice of rulemaking on this issue.

Intuit is providing its comments in writing and also by email to **GLB501Rule@ftc.gov**

Before commenting on the questions in the request for comment deemed relevant to Intuit, we offer our general comments on the development of the FTC Safeguards Rule. These general comments are applicable to all our specific responses in connection with the Proposed Rule, and include principles that we believe should guide the FTC in drafting the final Rule.

Please note that we have paraphrased the questions posed in the Proposed Rule for brevity of response, and while we addressed the majority of the questions posed, we have answered only those deemed most important and relevant to Intuit.

General Comments

As stated in our previous comment letter, Intuit believes the following principles should continue to guide the FTC in drafting its final Rule[1]:

- The FTC Safeguards Rule should provide sufficient flexibility for financial institutions to develop their own procedures to safeguard customer information.

- The FTC Safeguards Rule should apply equally to all financial institutions, regardless of their size, and to all assets equally. We believe that the FTC Safeguards Rule should focus on the sensitivity of the customer data being handled, and not on the size, complexity, or nature of the business handling it.

- The FTC Safeguards Rule should not establish specific procedures or methods for information security, but rather, permit financial institutions to change their security procedures to accommodate: (i) technological changes; (ii) social changes (including changed security risks); (iii) advances in business knowledge; and (iv) their own experience.

Further, we believe the FTC Safeguards Rule should track the guidelines of other financial institution regulatory agencies, to minimize differences in the standards of appropriate security procedures among different types of information holders. Financial institutions and other commercial enterprises may be regulated by more than one agency. Contradictory or inconsistent security requirements would lead to significantly higher costs of compliance and widespread confusion on the part of both businesses and the public.

Comments on Specific Questions:

§314.1 Purpose and Scope

Does including recipient financial institutions in the scope impose too great a burden? What about non-financial affiliates?

Inclusion of recipient financial institutions in the scope of the rule does not impose too great a burden on the recipients or on those who disclose customer records and information. This scope merely applies the "weakest link" theory of security, i.e., if data is to be protected, it must be protected at all points. However, the exact methods and technologies employed to protect customer data may reasonably vary from institution to institution. It is Intuit's position that the

[1] "Gramm-Leach-Bliley Privacy Safeguards Rule, 16 CFR Part 313 – Comment," Intuit Inc. (October 24, 2000).

FTC Safeguards Rule should set standards for the security of customer records and information, but not impose specific procedures or technologies of any particular type of institution.

Should compliance with alternative standards (e.g., SEC) constitute compliance with this FTC Safeguards Rule? If not, what procedures can be defined to avoid duplicating existing requirements?

Intuit believes that it is essential for the FTC Safeguards Rule to track the guidelines of other regulatory agencies. If, having done this, it develops that different agencies having jurisdiction over a single institution have inconsistent standards, then for the purpose of compliance, an institution's compliance with equivalent standards that apply to it should be deemed compliance with FTC's Safeguards Rule. Avoiding inconsistency and providing reasonably clear requirements to businesses is another reason why the FTC Safeguards Rule should be expressed as guidelines, rather than specific steps or procedures. To guide businesses in their security planning, it would be helpful for the FTC to issue a list of alternative standards which it considers to be "equal to or better than" its own, and accept conformance to any of these standards as conformance to its FTC Safeguards Rule.

§314.2 Definitions

What compliance burdens does this proposal place on entities, especially those which are already covered by safeguard standards of another agency?

Assuming the FTC adopts Intuit's recommendations, as discussed in the preceding question, the compliance burden for those entities covered by safeguards standards of another agency would be minimal, and could consist simply of an affidavit that the entity conforms to one or more of the sets of regulations that the FTC has defined to be "equal to or better than" its own. To the extent that the FTC adopts specific standards, procedures or technology requirements that conflict with, or exceed, those of other agencies, the compliance burdens would increase significantly.

Is additional guidance needed on what safeguards are appropriate for non-financial affiliates?

As stated above, Intuit believes that it is the nature of the data, not the nature of the affiliate, that should dictate the appropriate standard to apply to protect the data. The FTC might suggest possible ways for non-financial entities to abide by the principles set forth in the FTC Safeguards Rule, but these should be expressed as suggestions, not requirements.

Is the limitation to "customer information," where "customer" is defined as in GLB §501 to exclude "consumers," reasonable? Will financial institutions be able to distinguish between "customer information" and "consumer information"? Will consumers understand the distinction?

Intuit believes that the sensitivity of the data handled should be the distinguishing factor for purposes of whether it is subject to the safeguards rule, and not whether the data is that of customers or consumers. However, the FTC Safeguards Rule should adopt the same definitions as those used by other agencies in similar rules, wherever possible, as this will minimize both cost of compliance and consumer confusion. That said, if the FTC rule intends a different meaning for a term that is used by other agencies then the FTC should adopt a different term to avoid potential confusion.

The definitions of "information security program" is similar to the Banking Agency Guidelines' definition of "customer information system," and the definition of "service provider" is almost identical to the same definition in the Banking Agency Guidelines. Are these appropriate for the proposed FTC Safeguard Rule?

Again, consistency should rule: Unless there is an overriding reason to distinguish two terms, the same definitions should be used by all agencies. It is particularly unwise to use the same term to mean different things, so the definition of "service provider" should be standardized between the FTC and the Banking Agency Guidelines if possible; if this is not possible, the FTC should employ an entirely different term.

314.3 Standards for Safeguarding Customer Information

Does requiring a "written" information security program impose a disproportionate burden on smaller entities? Is there a way to lessen the burden of this requirement while still requiring each financial institution to develop, and be accountable for, an effective information security program?

Intuit believes that written documentation is critical for information security programs to be effectively implemented and managed over time. As long as "written" does not imply either a specific form or a single document, but could consist of (for example) Web pages or collections of multiple policies, procedures, or standards, the requirement that the information security program be "written" need not impose an onerous burden on any entity.

314.4 Elements

Does the requirement for a Single Point of Contact ("SPOC") (which can be any responsible employee or team, and which need not report to the Board of Directors as required by the Banking Agency Guidelines) impose too burdensome, too loose, or an appropriate level of accountability? Are there effective alternatives?

Intuit strongly supports the concept of SPOC for security-related issues. Different entities have different structures and make decisions at different levels. While it may be appropriate for financial institutions to assign the SPOC role to someone reporting to the Board of Directors, the wider variety of entities covered by the FTC Safeguard Rule make such a requirement impractical. We believe the FTC has taken the appropriate path in its SPOC requirement.

Is the requirement to "identify reasonably foreseeable risks" to the "security, confidentiality, and integrity of customer information" that could result in "unauthorized disclosure, misuse, alteration, destruction, or other compromise" of this information too burdensome, too specific, or not specific enough?

Intuit believes that this is just right, not too burdensome and sufficiently specific.

Is the requirement to consider risks in the areas of "employee training and management, information systems, and prevention and response measures for attacks, intrusion, and other system failures," too specific? Would additional guidance be useful?

Enumerating the areas mentioned is useful as guidance, but these areas should not be cast as a definitive list of specific areas in which risk must be assessed. For example, risk assessment in the area of "employee training and management" is vital for a large company with significant employee turnover, but may represent minimal risk to a very small or closely-held entity. The Safeguards Rule should give examples of risk assessment areas, but should not require specific areas to be covered.

Is the requirement to "regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures" (without specifying the particular audits or tests to be performed) too burdensome? Is it effective? What other concerns does this raise?

Every security system must be evaluated periodically, as new risks are discovered or other environmental factors change. Intuit strongly supports the need to "regularly test or otherwise monitor" the effectiveness of security systems. At the same time, the FTC Safeguards Rule should not require specific tests or monitoring procedures, as the cost-effectiveness of a particular test or monitoring procedure will vary greatly depending on such factors as the size of the entity, the nature of the business, and the technology employed.

Is a contract provision (between a financial institution and a service provider) necessary to protect customer information, or is there another, equally effective alternative? If a service provider is itself a financial institution or is otherwise subject to other safeguard standards, should there be an exception to the contract requirement?

A requirement to ensure that Service Providers protect customer information "by contract" is acceptable provided that the term "contract" is broadly used to mean the agreement between the financial institution and the service provider, and not any particular form of contract.

Should the FTC Safeguards Rule apply to all service providers, given that the Privacy Rule does not require financial institutions to have confidentiality contracts with service providers exempted by Sections 313.14 and 313.15 of the Privacy Rule?

As stated above, the FTC Safeguards Rule should apply to all entities that handle data needing protection, based on the nature and sensitivity of the customer data they handle. The FTC should regulate the security programs of all types of institutions over which it has jurisdiction, equally. Otherwise, certain institutions will bear the burden of information security while others do not. Likewise, if the FTC relies on regulated institutions to enforce the security concerns of those with whom they deal (e.g., by contract), then the FTC puts those institutions in the awkward position of being potentially liable for information security breaches of those parties with whom they deal. Intuit believes that the FTC Safeguards Rule should seek to minimize the differences in information security standards among the various types of institutions that handle protected data.

It is possible that a service provider could be subject both to the FTC's Safeguards Rule and to the Banking Agency Guidelines. Will complying simultaneously with these two sets of requirements pose any problems?

As indicated above, if an institution is subject to more than one set of rules or standards for information security, the FTC's position should be that compliance with one of those standards constitutes compliance with the FTC's Safeguards Rule.

Is the requirement to "evaluate and adjust [the financial institution's] security program" in the light of material changes to its business, too burdensome?

Intuit believes that evaluation and adjustment of an entity's security program should occur in response to material changes in the nature and sensitivity of the customer data being handled and changes in the nature of threats to information security, which may or may not coincide with changes in the financial institution's business. Changes in the financial institution's business, as expressed in the commentary in the Proposed Rule, focus on organizational changes such as mergers and acquisitions, alliances and joint ventures and the like. However, other changes are equally pertinent to the need for reevaluation of a security program, such as changes in product mix, changes in the nature of external threats, and so forth. Therefore, a general requirement to evaluate and adjust the security program should be included in the FTC Safeguards Rule, but it should not be dependent upon, or required to coincide with changes in the institution's business.

314.5 Effective Date

Is one year enough time to comply with the FTC Safeguards Rule? Should there be a transition period for "grandfathered" contracts?

Intuit is comfortable with a one-year effective date for new agreements. In the case of existing agreements, Intuit agrees with the FTC's suggestion in the Proposed Rule that a provision paralleling section FTC 16 CFR 313.18(c) would be appropriate:

> Two-year grandfathering of service agreements. Until <Rule date + 2 years>, an agreement that you have entered into with a nonaffiliated third party to perform services for you or functions on your behalf satisfies the provisions of Sec. 314.4(d)(2) of this part,

> even if the contract does not include a requirement that the third party implement safeguards to protect nonpublic personal information, as long as you entered into the contract on or before <Rule date>.

Intuit appreciates the opportunity to comment on the proposed FTC Safeguards Rule and would be happy to discuss further its concerns, comments, or other aspects of the Rule.

Sincerely,

James D Trovato Jr alw

James D. Trovato, Jr.
Director, Corporate Information Security