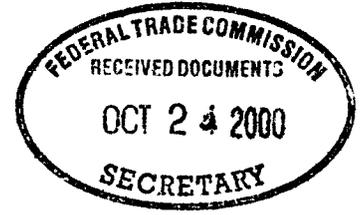




P.O. Box 7850  
Mail Station 2700  
Mountain View CA 94039-7850



October 24, 2000

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

**VIA HAND DELIVERY AND VIA EMAIL TO [GLB501Rule@ftc.gov](mailto:GLB501Rule@ftc.gov)**

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

Ladies and Gentlemen:

Intuit Inc. ("Intuit," [www.intuit.com](http://www.intuit.com)), 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, at [www.quicken.com](http://www.quicken.com), offering mortgage loans through its QuickenLoans website. Intuit also has 13 other websites which reach a large customer base. Intuit's 17 years' experience in handling and securing customer data makes the company specially qualified to address the issue of safeguarding customer privacy.

Intuit appreciates the opportunity to submit comments on development of the FTC's Safeguards Rule ("Rule") under Section 501(b) of the Gramm-Leach-Bliley Act ("GLB Act") as requested in its advance notice of proposed rulemaking and request for comment ("ANPR").<sup>1</sup> Intuit is providing its comments in writing and also by email to [GLB501Rule@ftc.gov](mailto:GLB501Rule@ftc.gov).

The FTC Safeguards Rule will provide safeguards for the customer records of financial institutions subject to the FTC's jurisdiction. Before commenting on those of the questions in the ANPR deemed relevant to Intuit, we offer our general comments on the development of the Rule. These general comments are applicable to all our specific responses to the ANPR's questions, and include principles that we believe should guide the FTC in drafting the Rule.

Please note that we have paraphrased the questions posed in the ANPR 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.

---

<sup>1</sup> 65 *Federal Register* 54186-54189, September 7, 2000.

## General Comments

In Intuit's view, the most important principle to be observed in developing the Rule is the retention of flexibility by financial institutions to develop their own procedures to safeguard customer information. For this reason, the Rule should be the same or substantially similar to the Interagency Guidelines,<sup>2</sup> which permit flexibility in the development of appropriate information security programs by depository institutions. We believe that differences in safeguard standards for customer records will be minimized among different types of financial institutions if the requirements for security programs are similar. Minimizing such differences will benefit both consumers and information-holders. Consumers will have confidence that appropriate security standards apply to all types of institutions that hold their personal information, and institutions will be able to better plan and execute their information security programs. Likewise, vendors of security products and services should be able to offer lower prices and more rapid product enhancements if a larger market follows the same rules.

Second, the Rule should apply equally to all financial institutions, regardless of their size, and to all assets equally. Customer information held by a financial institution is no less deserving of care or security because the institution is small or because the customer's account value is small. If the Rule specifies high level processes and requires specified levels of effectiveness, rather than specific methods and techniques, small financial institutions can develop security procedures appropriate to their size and their records.

Third, the 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. If specific technologies or methodologies are included in the Rule, scientific, social and business developments may make the Rule prematurely obsolete, or require its frequent revision. If unexpected challenges to information security emerge while specific processes are incorporated in the Rule, financial institutions could be burdened with inappropriate and potentially ineffective methods of providing information security.

To sum up our general comments, then, we believe the Rule should: (1) preserve to the financial institutions involved the flexibility to develop information security programs appropriate to their operations; (2) 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; (3) be uniform in its application to financial institutions and customer information, regardless of the institution's size or the assets involved; and (4) allow for changes in security procedures,

---

<sup>2</sup> Referring to the Interagency Guidelines of the OCC, Federal Reserve Board, OTS and FDIC.

methods and technologies as warranted by social, scientific, business and legal developments.

The merits of this approach are clear. Flexible guidelines can be implemented by financial institutions more quickly than detailed procedures, particularly by companies such as Intuit, that already have substantial information security programs in place. Prompt implementation of appropriate security procedures will further the FTC's goals in establishing the Rule while simultaneously benefiting the public and creating a predictable, achievable security environment for the financial services industry.

Comments on specific questions:

1. Scope of the Commission's Safeguards Rule

Section B.1 – Range of Information Subject to Rule

*Should the definition of "customer records and information" under the Rule be similar to the definition of "nonpublic personal information" for customers under the Privacy Rule?*

The Rule will be easier to follow (and provide more confidence for the customers of financial institutions) if its definitions are easily understood in the context of other FTC rules, such as the Privacy Rule. However, the term "customer records and information" may include public information as well as nonpublic personal information. In Intuit's case, some information provided by customers for financial transactions is available in public records (such as the information to refinance an existing mortgage, for example). Therefore, we believe that "customer records and information" should not be defined as "customer nonpublic personal information" unless those records contain only nonpublic personal information of customers. This presumes that a record-holder is able to segregate customer nonpublic personal information from publicly available information.

However, if a company chooses not to (or cannot) segregate customers' public and nonpublic personal information, it is appropriate to apply the same safeguards to protect both types of information.

Section B.2 – Range of Financial Institutions Subject to Rule

*How should the Rule apply when a financial institution discloses customer records and information to a financial institution that has no customer relationships or consumers?*

Disclosure of customer records and information to another financial institution should be subject to an agreement requiring the recipient to maintain appropriate safeguards to protect the information. If the Rule is drafted as a standard for records

security (and not as specific procedures), it could be applied to the recipient institution's handling of the information.

### Other Aspects of the Rule

*In what ways should the Rule take into account the need for financial institutions to keep pace with changing technology and other operational changes?*

It is vital that the Rule allow flexibility for a company to keep pace with changing technology and business needs. The Rule could achieve this by adopting the same standards as the Interagency Rule, i.e., by providing for regular evaluations of business changes and adjustment of security procedures. Technology choices and business methods must be flexible, not fixed in advance, or the Rule will quickly become obsolete. Likewise, the risks and threats to information security are constantly subject to change; for the Rule to be effective, it must encourage (indeed, require) information security programs to respond to these changes.

*Should the Rule specify minimum procedures for safeguarding customer records, minimum effectiveness, or both?*

Both. However, procedures specified in the Rule should not be detailed, and should be similar to procedures specified by the other financial institution regulatory agencies. Mandating effectiveness or results rather than detailed procedures allows industry to keep pace with technology.

*Do any current private standards, association rules, or guides provide useful guidance to the Commission?*

Yes. The following organizations have standards and guidelines; much of their information is publicly available. This is the type of information that an institution subject to security safeguards should be aware of.

CERT/CA ([www.cert.org](http://www.cert.org)) has several web pages covering recommended procedures for securing Unix and Windows NT systems and detecting and responding to security incidents. CERT/CA and other incident response teams have large archives of vulnerabilities that can be fixed in systems to protect consumer records.

In addition, the Department of Energy Computer Incident Advisory Capability (CIAC) and the International Computer Security Association (ICSA, [www.icsa.net](http://www.icsa.net)) have useful guidelines. There are also several Internet security assurance services available, including WebTrust (offered by the AICPA and VeriSign, [www.aicpa.org/webtrust/princrit.htm](http://www.aicpa.org/webtrust/princrit.htm)). Virtually all computer makers have web pages which identify vulnerabilities for their systems, which should be familiar to their users.

*Should the Safeguards Rule delineate mechanisms for financial institutions to demonstrate compliance with the Rule?*

Yes, if the mechanisms (1) require a demonstration of compliance with criteria appropriate to the specific institution's business activities, and (2) are illustrative but not mandatory. Examples of methods that may be used to demonstrate compliance include:

- (1) Automated security tests run internally by the company ("random but targeted testing");
- (2) Routine perimeter tests conducted by an independent auditor who makes an assessment about the robustness of monitoring and detection systems used to detect exceptions ("black box testing");
- (3) Creation of a security policy which an auditor tests to determine if the company is in substantial compliance with the policy ("white box testing"); and
- (4) Random inspection by internal and/or independent auditors to demonstrate the effectiveness of the company's safeguard policies and procedures (combination of "white box," "black box," and "random testing").

*Should the Safeguards Rule require financial institutions to use a particular audit process to measure its compliance?*

The Rule should allow financial institutions to establish their own audit processes for compliance measurement. Possibly, a spectrum of audit processes could be identified as illustrative in the Rule, including the following:

- (1) Routine tests of Internet perimeter testing (narrow auditing.)
- (2) Creation of a series of security assertions (i.e., policies) with an auditor's attestation of substantial compliance.
- (3) Demonstration of compliance with banking, brokerage, or other regulatory guidelines for a period of time, with the assistance of an independent auditor (i.e., in the manner of a SAS-70 audit).

*Should the requirements of the Rule apply to small financial institutions?*

Consideration of this question requires more information on what is meant by "small." Small could refer to number of employees, revenues, value of assets or other metrics. Intuit recommends that the Rule specify high level procedures for all financial institutions, so all customer information is subject to secure handling.

#### Specificity of the Safeguards Rule.

*What specific steps, if any, should the Rule require financial institutions to take to safeguard their customer records and information?*

The FTC should not attempt to create a master security policy for financial institutions. Rather than mandating specific safeguard steps, the Rule should provide a general framework around which companies can construct their security policies. In developing the Rule, the FTC must bear in mind that many mature companies, including Intuit, already have significant security procedures in place for customer information and

records, and they should not be required to scrap these policies and begin anew. A rule that promotes a framework will allow the security function to be uniformly maintained by all types of financial institutions with the likelihood that no industry sector will be much less secure than others.

*Is a different level of specificity appropriate according to whether the Rule is prescribing administrative, technical, or physical measures?*

Our view is that the Rule should not include specific measures, regardless of whether they are administrative, technical or physical. Detailed specifications tend to become outdated quickly and are more difficult to adapt to institutions of various sizes. Also, technical and physical security procedures cannot be meaningfully separated from administrative security procedures because administrative functions guide the development of all security measures. Rather than establishing specific measures, the Rule should describe the elements of a comprehensive security program, along the lines of Section III.C of the Interagency Guidelines.

*Should the Rule require financial institutions to take minimum steps, such as designating an employee responsible for monitoring internal access to customer records and information?*

Detailed requirements tend to become outdated, and are more difficult for companies to comply with, particularly if they are inconsistent with existing security procedures. For these reasons, Intuit favors a general framework rather than mandatory procedures and methods. However, if each financial institution is required to have a security "point of contact," administrative accountability will be enhanced. Auditing might also be an appropriate minimum step, but Intuit recommends that both identification of individuals or offices responsible for security and auditing be identified as suggestions or examples, and not required steps.

*Should the Rule set forth a more general standard for adequate safeguards, such as "effective controls or programs" or "reasonable policies and procedures"?*

Yes. Intuit feels that common and general standards are preferred to specific methods and procedures. It would be helpful to many institutions to have examples of adequate safeguards included in the Rule, but these should be identified as such. The ultimate goal of the Rule is effective controls; these can be achieved with reasonable policies and procedures. The specific steps that constitute reasonable policies and procedures, however, will change over time and with technological developments.

*If the Rule provides a general standard, what examples of adequate safeguards should be included?*

Certain examples could be included in the Rule for physical safeguards, such as shredding paper, or secure deletion of disk space. However, we believe it should be up to

the financial institution to determine what safeguards are adequate for it, based on its activities, its records, and its existing security programs and methods.

*Would safeguards categories that require financial institutions to focus on particular areas of operations, such as "Personnel Training and Management," "Information Storage and Transmission," and "Records Disposal," assist them in developing and maintaining thorough and consistent safeguards?*

The identification of categories could be helpful, particularly to institutions that do not presently have significant information security programs in place. However, a requirement to focus on particular areas would not be in the best interest of the FTC or the industry, as there is a possibility that certain categories could be overlooked, or the relative importance of the categories could be misunderstood by financial institutions. In addition, the categories of an effective information security program are subject to change as the institution's business changes. Specific identification of categories could therefore make the Rule obsolete unless the identification is expressly noted to be illustrative and not all-inclusive.

*Would a common standard, such as "effective controls or programs" or "reasonable policies and procedures" apply to every safeguards category, or should some categories, such as "Records Disposal," be subject to more objective requirements?*

Common standards are preferred for all categories. If objective requirements and actions are specified, there will be a temptation to conclude that if those actions are always performed, the company will always be in compliance and information will always be secure. Objective requirements could create new industry-wide vulnerabilities if companies merely follow those objective requirements without regard to whether they are effective.

### Statutory Objectives.

a. Anticipation of Threats or Hazards

*Should "anticipated threats and hazards" be defined in the Rule, and if so, how?*

Specific types of anticipated threats and hazards could be illustrated, but should not be defined in the Rule. Defining threats and hazards is an effort doomed to fail because new ones are always emerging. In addition, different types of threats and risks face different types of financial institutions. Many institutions already have experience with known risks and threats, while others, particularly financial institutions that are just going online, may have little or none. The processes for assessing risk are dependent on what kind of financial institution is involved, what types of systems it uses, and what kinds of records and information it has. Therefore, Intuit recommends that the Rule

include a list of possible threats and hazards, without limiting the definition of the term to the items on the list.

Among the anticipated threats and risks that could be included as illustrative in the Rule, and for which an effective security program will have procedures, are:

- ◆ Risks of unavailability (denial of service)
- ◆ Programmatic risks (arising from unexpected inputs, such as application development or design errors).
- ◆ Platform risks (arising from security vulnerabilities within the computing platform on which the system operates)
- ◆ Network risks (arising from rerouting traffic, bypassing network access controls, or by exploiting vulnerabilities in the networking infrastructure)
- ◆ Physical access risks (created by an attacker with physical access to the systems)

In addition, threats could also be defined in terms of the assets being protected, including:

- ◆ Threats to customer identity
- ◆ Threats to customer privacy
- ◆ Threats to the integrity of customer information

and they could be defined by the source of the threat, such as:

- ◆ Threats from attackers from outside the company
- ◆ Threats from insiders
- ◆ Threats from organized attackers with or without significant resources
- ◆ Threats from industrial competitors

Just these few alternatives should make clear that defining anticipated threats and risks in a closed-end manner is likely to be incomplete and may reduce the creativity that leads companies to develop wide-ranging information security programs.

*Should the Rule require financial institutions to anticipate threats and hazards according to particular procedures?*

No; the Rule should not require financial institutions to anticipate risk using specific procedures. Many financial institutions do use specific procedures, but identifying these in a Rule that applies to a wide variety of financial institutions will result in procedures that are appropriate for some but inappropriate for others. In addition, the actuality of responding to risks and threats over time helps companies refine and modify their risk assessment procedures. Thus, risk assessment procedures themselves are constantly evolving and would be difficult to capture in a Rule in a current manner without the need for constant rewriting of the Rule. Financial institutions should be free to use procedures appropriate for their operations to anticipate risks.

*Should the Rule require financial institutions to assess threats and hazards according to particular categories such as "Risks to Physical Security," "Risks to Integrity," or "Risks in Records Disposal"?*

No; for the same reasons we identified above in response to the question whether the Rule should focus on specific categories for safeguards in operations. Risks and threats are constantly emerging; assessing risk by pre-defined category may lead to the result that new and unforeseen categories of risk that arise in the future are not part of the risk assessment procedure specified by Rule.

*When assessing threats and hazards, should a financial institution be required to classify the value and sensitivity of the records to be protected and/or the gravity of any threats?*

Not all protected information has calculable monetary value. If the value of a financial account determined the processes used to secure it, high value accounts would be more carefully secured than modest accounts, which we believe is unfair to customers. Certain types of information are probably generally acknowledged as deserving of particular security, however, such as medical information, social security numbers and the like. We believe that industry will develop appropriate conventions for protection of highly sensitive information. We urge the FTC to permit financial institutions to develop their own methodologies for risk assessment in light of their particular operations and records.

*Under what circumstances, if any, should financial institutions be required to conduct these assessments in writing?*

We expect that financial institutions will maintain records of their risk assessment procedures, but would not favor a rule requiring the assessments themselves to be reduced to writing. Risk assessment, like other methods of compliance self-testing, has the potential to be used against the company that is assessing the risk. This potential could have the effect of causing companies to minimize their efforts to assess risk. This would be counterproductive to the purposes of the Rule. In addition, written records of security assessments should be treated as extremely sensitive. There is potential for abuse if written records of assessments are made public prior to the time vulnerabilities in a system have been corrected or fixed.

*Should the Rule require financial institutions to reassess threats or hazards to their information security systems, and, if so, at what intervals?*

Financial institutions should reassess threats to their operations and information security programs periodically. However, the specific interval should not be subject to a hard and fast rule. Different types of institutions have different needs for reassessment, based on several factors, including how often they change systems, how often they change their product mix, whether they do business with new partners, how fast their business (and volume of customer records) grows, and so forth. There is no one set

interval that will be appropriate for all institutions. The Rule could suggest an interval for reassessment, such as every calendar year, but it should provide flexibility for more or less frequent reassessments based on factors appropriate to the institution's business.

*Should the Rule define technical or other changes to an institution's information security environment that warrant reevaluation of existing safeguards?*

As indicated above, there are a variety of factors that could warrant reevaluation of a security system. To attempt to enumerate all the factors would probably be futile. We recommend that the Rule include examples of the types of changes to operating environments that warrant reevaluation. For example,

- ◆ changes to operating software in firewalls, or routers operating within the network,
- ◆ changes to authentication and access control systems
- ◆ staff changes, departing employee access review
- ◆ security advisories released by credible sources

Companies should be free to add to these factors, or to weigh the various factors in determining whether reevaluation is appropriate, as appropriate to their business.

*Should a financial institution be required to assess threats and hazards within a reasonable time after it knows of a new or emerging threat to the security or integrity of its records?*

Yes, but the time should be specified as "reasonable," without a specific time frame for response.

*Should the Rule require that the effectiveness of existing safeguards be evaluated through appropriate tests? How should the standards define these tests?*

As a practical matter, the effectiveness of safeguards should be evaluated by testing. However, if information security safeguards are formally adopted but not put into practice, testing will be ineffective. The effectiveness of an institution's safeguards cannot be assumed merely because testing does not reveal deficiencies or exceptions. If the standards define the tests, companies can work around the safeguards by complying with the precise elements of an information security plan that will enable them to pass the tests. This could result in less effective security programs. Therefore, although we favor testing to determine effectiveness, we do not believe the testing standards should be part of the Rule.

*How should the Rule protect against anticipated threats and hazards to the integrity of customer records and information?*

The Rule can protect against anticipated threats and hazards to customer records by permitting, in some instances, customers to control their information. For example, if

a customer wants his or her information to be deleted from an institution's records, the Rule could require that it be erased securely, provided there is no legal requirement to keep the records.

However, a rule cannot protect the integrity of customer records if financial institutions do not comply with the rule, or if they do not have bullet-proof information security programs. The ability of hackers to violate seemingly secure websites demonstrates that there is no guarantee of integrity or security of customer records, regardless of the good intentions of the financial institution and the government. The best that the Rule can do is to require reasonable information security programs, provide for investigations and sanctions in case of willful non-compliance, and avoid the creation of a public impression that information provided to financial institutions is somehow excepted from the normal incidents of human error.

*Should protecting integrity of customer records and information include requiring a financial institution to notify customers when records and information are subject to loss, damage, or unauthorized access?*

No. There may be instances when unauthorized access to customer information does not result in a loss or harm to customers, although it does violate the financial institution's information security program. Likewise, in the case of loss, the customer might not be harmed; indeed, it could be the financial institution that is harmed, based on loss of valuable data. We believe that a better requirement would be for institutions to notify customers if they have reason to believe that harm or damage was actually done. Otherwise, customers will be unnecessarily worried if they receive notices that describe "maybe" situations. For example, if a secure door is inadvertently left unlocked, there could be unauthorized access to an area where customer private information is stored. However, the fact that the door was unsecured does not necessarily mean that unauthorized access has occurred, or that any customer was harmed.

Another reason for not requiring notices of merely potential unauthorized access situations is that a cottage industry of class action litigation could arise based on these notices.

*Does insuring integrity of customer records and information require that customers be granted periodic access to their records, in order to monitor its accuracy?*

We believe that granting customers access to their records should be left to the discretion of the financial institution involved. Although accuracy is critical to the appropriate use of customer information, many companies might not be set up to handle customer inquiries concerning the accuracy of their information. (Likewise, the source of some of the information in the records of financial institutions may be unknown.) In addition, there may be insufficient sources of information available to the financial institution to verify the accuracy of information disputed by the customer. Information that a customer claims is inaccurate might be accurate. The financial institution should

not have to enter the data verification business in order to use its own records. However, we do not object to the encouragement (in the Rule) of financial institutions to grant records access to customers. In the future, customers might make their selection of financial institutions based on whether the institution provides access and data correction capability.

Preventing Unwarranted Access and Use.

*Should "unauthorized access" and "unauthorized use" be defined, and if so, how?*

“Unauthorized access” and “unauthorized use” should be defined as any access or use of customer information outside of the financial institution’s security program.

*Should the Rule require financial institutions to follow certain minimum procedures to protect against unauthorized access to customer records and information?*

The Rule should not specify minimum procedures for preventing unauthorized access, but should state that an information security program should contain procedures for preventing unauthorized access. The rules of access for different financial institutions will be different, based on factors such as their physical premises, their operating systems, the number of their employees, and the like. To specify minimum procedures will likely lead to a low level procedure which is realizable for smaller institutions but insufficient for larger institutions. Alternatively, if highly detailed, the procedures could be impossible to follow, or prohibitively expensive, for smaller institutions.

*Should financial institutions be required to maintain written records of their procedures for preventing unauthorized access and use?*

As indicated above, we believe that as a practical matter, financial institutions will document their procedures in some form (otherwise, it would be difficult to inform the employee population about the access policy) but that it should be up to them how to do this. A specific requirement for written records could inhibit the reevaluation and modification of the access policy as often as it should be reevaluated and modified. (Once something is written down, it can tend to become “fixed” and inalterable.) Security procedures should be treated as extremely sensitive information of the company and be protected from unnecessary disclosure, to protect both the company and the integrity of the information being protected by the security program.

*Should the Rule require financial institutions to designate a person responsible for preventing and detecting unauthorized access to and use of customer records and information? Should the Rule require financial institutions to enter into confidentiality agreements with employees or train them in preventing unauthorized access?*

The Rule should not require the designation of a person for specific tasks in information security management, although as a practical matter many companies might

do this. The prevention of unauthorized access should be part of the information security program, but our view is that the implementation of the program should be left to the company, provided it meets the FTC's standards for effectiveness and reasonableness, and the company can demonstrate its compliance.

Likewise, with employee training, we think this is likely to occur as an element of an effective information security program. However, we do not agree that the Rule should be at the level of detail where employee agreements are required or where employee training programs are required. In many situations, employees work without benefit of employment agreements, and to introduce agreements on one subject might open the door to significant legal question about why other aspects of the employment relationship are not addressed. This could have unforeseen implications for a financial institution's labor relations. Similarly, in some smaller financial institutions, there may be no formal training programs, but on-the-job training might be used. We see no need for the FTC to mandate what types of employee training are required as part of the privacy implementation rule.

Insuring security and confidentiality.

*Does the requirement to insure the security and confidentiality of customer records and information mean something more than protecting against anticipated threats and hazards and unauthorized access and use?*

No. However, we again would caution that there is no "insurance" of the security and confidentiality of customer records, regardless of the eventual language of the Rule. We believe it would be misleading to consumers, and counterproductive, for the FTC to suggest otherwise, by the language of the Rule.

*In particular, what should ensuring "confidentiality" of information mean?*

Ensuring confidentiality should mean (within the meaning of the Rule) that a financial institution has taken reasonable measures to prevent a customer's private information from being used in a manner inconsistent with the customer's intentions. This means that the institution has adopted an information security program with meaningful steps of its own devising, to prevent the unintended use.

*What measures should the Rule require a financial institution to take to maintain the confidentiality and security of customer records and information that it discloses?*

The Rule should require a financial institution that discloses information to have as part of its information security program methods and processes for ascertaining that the recipient will protect the confidentiality and security of the records. This can be done by agreement.

*Should the Rule require a financial institution that discloses customer records and information to notify the recipients of the limitations on reuse and redisclosure of the information imposed by the Privacy Rule?*

Yes; we believe this is already a requirement imposed by the GLB privacy regulations.

#### Consideration of Other Agencies' Safeguards Standards.

*Should the Commission's Safeguards Rule be similar to the Interagency Guidelines, and if so, how?*

We believe, for the reasons set forth in this letter, that the Rule should be consistent with the Interagency Guidelines. The Guidelines are specific in their intent but allow financial institutions flexibility to achieve those intentions. This is necessary in light of the great variety of institutions that are subject to the FTC's jurisdiction. We also believe that similar requirements for information security programs across the financial industry is a worthy goal, as companies are merging and reorganizing daily. To the extent that a financial institution enters a new line of business or merges with another type of institution, its information security program will be more meaningful and constant if the rules across the industry are consistent. Consistent rules also lead to more consumer confidence in the marketplace.

*Does the Act's requirement that the Commission issue a rule, rather than guidelines, warrant a different approach?*

No. The Rule can be a guideline, or more practically, a requirement that financial institutions adopt a framework for information security programs.

*Does the fact that the Commission does not conduct regular examination of financial institutions warrant more specific security measures?*

No, in fact, the lack of regular examinations warrants precisely the contrary. To the extent the FTC does not examine the institutions subject to its jurisdiction generally, a specific rule will result in arbitrary enforcement of the requirement. Companies that choose to disregard the Rule (or that are unaware of it) may never be disciplined; their customers may suffer harm as a result of the lack of enforcement and the reputation of the FTC as an effective agency will suffer. Certain companies, aware of the limited enforcement resources and lack of examinations, may never adopt the procedures in a specifically drawn rule, but may adopt a more general framework for information security that is established in a more flexible guideline.

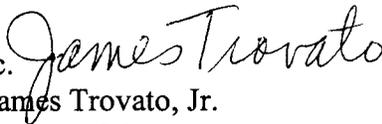
#### Conclusion

Although the GLB Act does not require the FTC to coordinate with other federal agencies in developing its Safeguard Rule, we urge the FTC to do so. The work that has

been done to date on developing information security safeguards for depository institutions is valuable and we believe it could be adopted with few or minor variations by institutions subject to the FTC's jurisdiction. If the Rule is consistent with the guidelines applicable to other financial institutions, a uniform standard for information security can be achieved across the financial services industry, and customers can be confident that their records and information are handled appropriately, regardless of the identity of the information-holder. The flexibility built into the Interagency Guidelines allows institutions of all sizes to develop information security programs appropriate to their size and resources. Finally, the Rule should contemplate adjustment of an institution's information security program and adoption of technological, methodological and procedural changes to keep the program current and effective.

As the Privacy Act and Safeguards Rule are new, it remains to be seen what challenges in information security will emerge in the financial services industry. We believe the initial Rule should therefore be broad, but also uniform, general and flexible, and that it should, like the processes it will engender, develop over time to reflect specific information security, social and business needs.

Respectfully submitted,

Intuit Inc.    
By: James Trovato, Jr.  
Its: Program Manager  
Information Security