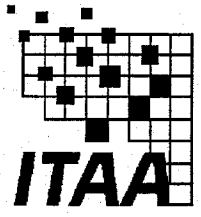


October 9, 2001

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

Re: "Gramm-Leach-Bliley Act Privacy Safeguards Rule, 16 CFR Part 314."

ITAA Comments

ITAA welcomes the opportunity to submit this letter in response to the FTC's proposed "Standards for Safeguarding Customer Information," published in the Federal Register on August 7, 2001. (66 FR 41162). The proposed rules, and the Gramm-Leach-Bliley Act ("GLB") (Public Law 106-102) under whose authority they have been issued, rest on the premise that a firm security foundation is a necessary prerequisite to protect the privacy of customer-related information of financial institutions.

The Information Technology Association of America (ITAA) provides global public policy, business networking, and national leadership to promote the continued rapid growth of the IT industry. ITAA consists of over 500 corporate members throughout the U.S., and a global network of 41 countries' IT associations. The Association plays the leading role in issues of IT industry concern including information security, taxes and finance policy, digital intellectual property protection, telecommunications competition, workforce and education, immigration, online privacy and consumer protection, government IT procurement, human resources and e-commerce policy. ITAA members range from the smallest IT start-ups to industry leaders in the Internet, software, IT services, ASP, digital content, systems integration, telecommunications, and enterprise solution fields. For more information visit www.itaa.org <http://www.itaa.org>.

ITAA supports the FTC's proposed rules. In particular, ITAA agrees that the security requirements adopted by the FTC under GLB should be flexible, technologically neutral, and appropriate to the data being held by each particular financial institution. However, the rules should clearly reflect that for the reasons stated below, the financial institution, not service providers, must be responsible for determining appropriate safeguards afforded to customer-related information of financial institutions.

Information Technology Association of America
1401 Wilson Blvd. # 1100 Arlington, VA 22209 • Ph: (703) 522-5055 Fax: (703) 525-2279

Customer-related information held by a financial institution will differ from entity to entity, as will the uses made of that information, but all institutions have in common a strong desire to protect such information from unauthorized or unlawful access and disclosure. Nowhere is protection of customer information more important than among financial institutions, where marketplace reputations are based upon the bedrock of such protection.

Each financial institution is in the best position to weigh the value and sensitivity of customer-related information. This weighing is done not only in connection with its own business, but also in the context of the legal requirements to protect such data imposed on it as an institution by the FTC and other regulatory authorities. Each such financial institution must assess the risk of loss or compromise of such data and is responsible to put in place appropriate measures to manage such risk, and to comply with statutory requirements. Such risk assessment and management is both a legal imperative and a marketplace necessity.

In order to become ever more competitive in the marketplace, enterprises, including financial institutions, continue to review and rework their business processes. The thoroughness of these reviews has resulted in changes of such magnitude that they are often described as "transformations." Such transformations may include, in part, outsourcing certain capabilities to third parties, such as clearing houses, transaction processors, service providers, and web hosting firms. Over time, even individual applications, storage of data, and other elements of data handling and processing may be outsourced.

Service providers, information technology and security companies, and others, should work with financial institutions to help the financial institution in its determination of what security implementation is appropriate to manage reasonably the security risks that have been assessed. Security requirements will vary based on business requirements (e.g. response time considerations) and other needs of the financial institution. As participants in the FTC's Advisory Committee on Access and Security have noted, security does not operate in a vacuum as an absolute value, but must be balanced against competing values. [1]

However, the financial institutions will, within the constraints of legal compliance, make the ultimate, appropriate choices about: various possible solutions, implementation costs, customer convenience, the necessity to maintain efficient operations, etc.

---

[1] Final Report of the FTC Advisory Committee on Online Access and Security May-15 2000, http://www.ftc.gov/acoas/papers/finalreport.htm

Under these circumstances and as directed by GLB, the FTC proposal that responsibility for compliance with security requirements lies with the financial institution which has the primary relationship with the customer whose data is being protected is entirely appropriate.

In addition, the security rules should be harmonized with the FTC's Final Privacy Rule.[2] The FTC has invited comment on this point asking "whether [proposed section 314.4(d)(2)] should apply to all service providers, given that the Privacy Rule does not require financial institutions to enter into confidentiality contracts with service providers that receive information under the general exceptions in sections 313.14 and 313.15 of that Rule." ITAA agrees with the implied logic of the FTC's question that where no confidentiality agreement is required under the Privacy Rule because the disclosures fall within the exceptions of sections 313.14 or 313.15, it is also inappropriate to require financial institutions to have contractual arrangements with service providers under the security safeguards rules for those same exempted disclosures. ITAA believes that the requirements of proposed section 314.4(d) should be modified accordingly.

Apart, potentially, from these limited situations, financial institutions will be connected contractually with their suppliers to provide mutually agreed to levels of service, including these security arrangements. Nevertheless the financial institution remains the logical focal point of control and responsibility in terms of the actual security needed to protect its customer data in accordance with statutory and other requirements.

In summary, and except as noted above, ITAA believes that the FTC's proposed rule 16 CFR 314.4(d) accurately captures this differentiation in roles between the financial institution and its suppliers:

- The financial institution "owns" the data being processed or stored and is ultimately the entity to which the FTC looks for legal compliance. The financial institution may not diminish or transfer this obligation by outsourcing the handling or storage of the information;

With any input it may solicit from its suppliers and consultants, the financial institution:

1. Determines what processes and elements and data it will handle in house, and what processes and applications will be out-sourced;
2. Does the risk assessment with respect to protecting its processes and data;

---

[2] 65 FR 33646 et seq., May 24, 2000

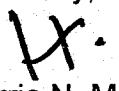
3. Determines the service levels and security implementations appropriate for its needs and necessary for its legal compliance;
4. Selects those suppliers it will use and enters into contractual arrangements with them to provide those levels of service and to implement the agreed upon levels of security for those outsourced services, or for the outsourced security aspects of processes and data which remain internal to the financial institution; And
5. The financial institution provides oversight of these suppliers.

This is consistent with the FTC's proposal and the GLB approach, that the financial institution should be the entity responsible for compliance with the FTC's GLB security requirements.

ITAA believes the approach adopted by GLB and the proposed rules gives financial institutions and their suppliers the flexibility they need to continue to transform their businesses while providing appropriate protection for customer-related information.

Thank you for your careful consideration of these important issues. If you have any questions about the matters raised above, please feel free to contact me (703/284-5340; hmiller@itaa.org), or Shannon Kellogg (703/284-5347; skellogg@itaa.org) of my staff.

Sincerely,



Harris N. Miller
President
ITAA