

October 9, 2001

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

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

Dear Sir or Madam:

Oracle wishes to thank the Federal Trade Commission (FTC) for the opportunity to comment on developing administrative, technical and physical information Safeguards Rule that the Commission is establishing pursuant to section 501(b) of the Gramm-Leach-Bliley (GLB) Act. Our clients represent a broad cross-section of financial services institutions and we are writing to provide comments on issues related to technical security requirements. As technology environment increases in complexity and network connectivity expands, the level of risk within organizations also increases.

**Section B, Question 2. Range of Financial Institutions Subject to the Safeguards Rule.**

Financial services institutions were broadly defined in GLB to include some companies that have no direct relationships with customers. It would neither be appropriate nor practical for those companies to have direct contact with the customers of the financial service institution. Most often they are engaged in supporting back end work and systems for which they have contractual relationships that bind them to act according to specified terms. Depending on the supporting work being performed by the other party, there may be need for more detail and direction than is provided for in the Safeguards rule, it may be best to merely suggest that contractual terms should appropriately reflect the security requirements that the financial institution desires that its contract parties adhere to.

**Section C**

In light of the breadth of the definition of financial services institution and the variety of existing systems and security deployments, it may be hard to delineate a specific set of ways to comply. Previous Government positions have been very careful to remain neutral

in terms of possible solutions, endorsing neither specific technologies nor implementations as a way to make sure that customers were provided with maximum choice in the market and the necessary flexibility to tailor solutions to their needs. There are, however, a number of private sector and technical standards bodies that are dedicated to the review and evaluation of specific products. There are numerous recognized certifications that attest to security, and more than one may provide the appropriate attestation of security. While we don't prejudge which certification is the most appropriate, we would suggest that recognized security certifications of products are one of the best and most objective external indicia which can be used to evaluate security.

**Section C, Question 2.**

Information security depends on a number of variables including the sensitivity of the information need for access, times, speed and of accesses as well as existing infrastructure. Administrative, technical and physical security must work together to provide security but may have very different levels and forms of implementation. At best guidance should indicate the need for companies to comprehensively review all three issues and develop complementary solutions to assure security. For example, one factor of the review and complementary solution may be whether the institution is the sole occupant or owner of the building. Where the building has multiple tenants the institution may not be able to restrict access to the extent it would like and may consider stronger safeguards both administratively and technologically. All institutions need to determine how to coordinate security. In some cases one person may be the appropriate point of responsibility, in others it may be a cross functional team. In all cases, however there must be a clear tasking of responsibility for these issues. In light of the need for complementary solutions and existing infrastructures, it may be difficult to specify what adequate safeguards are. A requirement for reasonable policies and procedures would seem appropriate, but may provide too little guidance for some. An approach of providing guidance by examples of categories of things that regulators may look for in reviews of adequacy may be the most instructive path forward without constraining the institution to any particular technology or implementation.

**Question 3A. Anticipation of Threats or Hazards to Security or Integrity.**

Threats remain an ever-changing phenomenon and there can be no really comprehensive list of threats that remain up to date—even for brief periods. Categories or general types of threats or risks, however, may be addressed. It is important that firms dealing with information understand the sensitivity or importance of the data they access. Without such an understanding it is impossible to determine what level of security is appropriate for the data in question or how to properly deploy security resources. It is important to note that sensitivity of data should not be confused with issues related to security of devices or access controls. Weak links in systems not protecting highly secure

information may still become pathways to compromise. Thus security must always be considered as a whole and not just a sum of parts.

The fast changing pace of innovation and deployment of threats requires firms to review their ability to respond to threats. These requirements to review threats are not necessarily in synch across the threats. There may be many new viruses, but the appropriate response is not continuously reviewing whether antivirus scans are the solution but rather a policy that assures that virus definitions are kept up to date.

**Question 3b. Preventing Unwarranted Access and Use.**

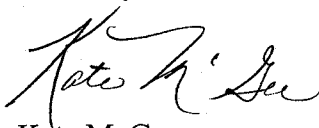
Addressing concepts of unwarranted access and use are somewhat counterintuitive. It is more commonplace for firms to define appropriate access and use; then provide for sanctions or consequences for acting outside the scope of accepted access and use.

**Question 3c. Insuring Security and Confidentiality.**

Many of the questions related to confidentiality are already dealt with under the privacy guidance that has been already provided. Rather than require that harmonization take place after drafting the guidance, it may be more straightforward cross-reference the actual privacy guidance.

Once again, Oracle appreciates the opportunity to comment on this very important matter. The advent of e-commerce and e-business presents exhilarating opportunities for the industry and consumers alike. The proposed rule's overall approach will encourage innovation and flexibility in the financial services industry while providing appropriate safeguards for customer data.

Sincerely,



Kate McGee  
Vice President  
Corporate Affairs