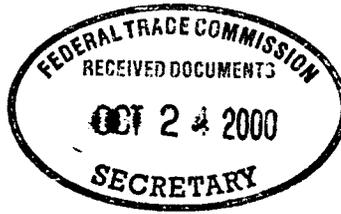


Noah J. Hanft
Senior Vice President
U.S. Region Counsel &
Assistant General Counsel

MasterCard International

Legal
2000 Purchase Street
Purchase, NY 10577-2509

914 249-5595
Fax 914 249-4261
E-mail noah_hanft@mastercard.com
Internet Home Page:
<http://www.mastercard.com>



*MasterCard
International*



Via Hand Delivery

October 24, 2000

Secretary
Federal Trade Commission
Room H-159
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Gramm-Leach-Bliley Act Privacy Safeguards Rule, 16 CFR Part 313—
Comment

Dear Mr. Secretary:

This comment letter is filed on behalf of MasterCard International Incorporated (“MasterCard”)¹ in response to the advance notice of proposed rulemaking (the “Notice”) published by the Federal Trade Commission (the “Commission”) requesting comment on developing an administrative, technical, and physical information safeguards rule.

MasterCard appreciates the opportunity to provide comments prior to the Commission issuing a proposed rule (the “Safeguards”). In particular, we applaud the Commission for its indication that it will consider the costs and benefits of the Safeguards’ requirements. Furthermore, we commend the Commission for recognizing that “financial institutions may deem different safeguards appropriate according to the size and complexity of the financial institution, the nature and scope of its activities, and the nature of its records.” This acknowledgement is critical and should be the fundamental principle for Safeguards which allow each financial institution to design an information security program that is best suited to the operations and activities of that financial institution. We offer the following more specific comments for consideration by the Commission when preparing the Safeguards as a proposed rule.

¹ MasterCard is a membership organization comprised of financial institutions which are licensed to use the MasterCard service marks in connection with payment systems, including credit cards, debit cards, smart cards and stored-value cards.

In General

The Commission has issued its Notice in response to section 501 of Title V of the Gramm-Leach-Bliley Act (the "GLB Act") which directs several federal agencies, including the Commission, to establish appropriate standards for use by financial institutions in safeguarding customer records and information. The Securities and Exchange Commission (the "SEC") issued standards for financial institutions within its jurisdiction as part of regulations implementing the privacy provisions of the GLB Act (the "Privacy Rule"). The federal banking agencies recently issued proposed standards in the form of guidelines (the "Banking Agency Guidelines").

Although the GLB Act requires the Commission's standards to be in the form of a rule, we would urge the Commission to issue Safeguards which grant financial institutions enough flexibility to allow for the rapid modifications needed to address new threats as they develop. In this regard, the Safeguards should give general direction to financial institutions while enabling each financial institution to develop policies and procedures best suited to its own operations and experiences. We urge the Commission not to propose standards or procedures which are more rigid than would be appropriate given the dynamic environment surrounding information technology.

Should the Commission choose to include more detail, it may wish to consider the Banking Agency Guidelines as a model. Although we provided several suggestions as to how the Banking Agency Guidelines could be improved, we believe that, in general, they were an effective approach to protecting information security. Key components of the Banking Agency Guidelines were derived from security-related supervisory guidance previously issued by the banking agencies and the Federal Financial Institutions Examination Council. This supervisory guidance has proven effective and addresses the issues required to be covered in the Safeguards.

Scope

The Commission has requested comment on issues related to the proper scope of the Safeguards. This includes determining the range of information, and the range of financial institutions, subject to the Safeguards.

Definition of "Customer" and "Consumer Records"

The Commission has requested guidance with respect to how the term "customer records and information" should be defined as part of the Safeguards. We believe the meaning for this term can be found in the GLB Act and the Privacy Rule. Section 501(b) of the GLB Act directs the Commission to establish standards for safeguarding records and information relating to "customers." Congress referred to "customers" in section 501(b), as opposed to using the term "consumers" as it did elsewhere in Title V of the GLB Act. The Commission recognized the significance of the distinction between the two terms in connection with the Privacy Rule. Specifically, in a discussion titled "Distinction Between 'Consumer' and 'Customer,'" the Supplementary Information to the Privacy Rule states that

“[t]he Commission believes . . . that the distinction [between ‘consumer’ and ‘customer’] was deliberate and that the [Privacy] [R]ule should implement it accordingly.” 65 Fed. Reg. 33,650 (May 24, 2000). The Supplementary Information explains that “[a] plain reading of the [GLB Act] supports the conclusion that Congress created one set of protections . . . for anyone who obtains a financial product or service [(i.e., “consumers”)] and an additional set of protections . . . for anyone who establishes a relationship of a more lasting nature than an isolated transaction with the financial institution [(i.e., “customers”).” *Id.* Congress made the same distinction when enacting section 501 of the GLB Act and limited that section to “customer” information. We urge the Commission to honor this distinction in the Safeguards.

The broader term of “customer records and information” is not defined in the GLB Act or the Privacy Rule. However, given the breadth of the Privacy Rule’s definition of “nonpublic personal information,” which includes “any information [a financial institution] obtain[s] about a customer in connection with providing a financial product or service,” we believe “nonpublic personal information” to be synonymous with “customer records and information.” 16 C.F.R. § 313.3(o)(1)(iii).

It is important that the definitions of “customer” and “customer information” be consistent with corresponding provisions set forth in the Privacy Rule. Financial institutions will be able to protect “customer” privacy most effectively only if they can readily determine which information is subject to both sets of requirements. Any suggestion that the term “customer” or “customer information” would have different meanings under the Safeguards and the Privacy Rule would create confusion and make it more difficult for the personnel who have primary responsibility for implementing the two rules to do so. Moreover, there is nothing in the GLB Act or its legislative history that would suggest that the terms “customer” or “customer information” should have different meanings under the Safeguards than they do under corresponding provisions of the Privacy Rule.

Consistent with the definition of “customer,” we would also urge the Commission to limit the Safeguards to cover information regarding customers who obtain financial products or services from a financial institution for “personal, family, or household purposes.” As the Commission acknowledged in the Privacy Rule, the privacy provisions included in the GLB Act apply “only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family, or household purposes . . . [and do] not apply to information about companies or about individuals who obtain financial products or services for business, commercial, or agricultural purposes.” 16 C.F.R. § 313.1(b). We urge the Commission to continue to use this approach by applying the Safeguards only to “customers” who obtain financial products or services for “personal, family, or household purposes.”

The Commission specifically asks whether the Safeguards should ever apply to *consumer* information. As discussed above, we believe the GLB Act limited the scope of the Safeguards to *customer* information. We acknowledge, however, that financial institutions may choose to develop security safeguards applicable to “consumers,” business clients, and other entities not covered under section 501 or the Privacy Rule. However, the GLB Act does not, and the Safeguards should not, *require* them to do so.

Range of "Financial Institutions" Subject to the Safeguards

The Commission has requested comment on the range of financial institutions to which the Safeguards should apply. Specifically, the Commission would like comment on how the Safeguards should apply when a financial institution discloses customer records and information to a financial institution that has no customer relationships. By definition, unless an individual has a continuing customer relationship with the financial institution, that individual is not the financial institution's customer. Since section 501 provides that the Safeguards are to apply to "customer . . . information," if an individual is not a financial institution's customer, the Safeguards do not apply with respect to any information related to such individual, even if in the possession of a financial institution.

We understand, however, the importance of maintaining the security of information given to third parties. To address this issue, the Commission should recognize that, where appropriate, financial institutions may utilize traditional means of restricting the information practices of service providers, such as by contractually imposing responsibility on service providers to employ proper information protections. Such contractual provisions can be used to enable financial institutions to take appropriate steps when weaknesses are detected in a service provider's security program or practices.

Standards for Safeguarding Customer Information

As noted above, we applaud the Commission for acknowledging that each financial institution may deem different safeguards appropriate according to the size and complexity of the financial institution and the nature of the information being protected. We believe this should be the fundamental and guiding principle of the Safeguards. For example, the Safeguards should provide several general options with respect to achieving a satisfactory level of security. If the Safeguards become too prescriptive, financial institutions may be forced to adopt standards and procedures which are inappropriate for the given financial institution. Furthermore, the Commission must provide financial institutions the flexibility to adapt to changes in technology and criminal behavior in the future. This type of approach is the foundation of the Banking Agency Guidelines, and we believe it would be the most effective.

Development and Implementation of Information Security Program

The Commission seeks comment on how the Safeguards should reflect the three statutory objectives for information safeguards: (1) anticipation of threats or hazards to security or integrity of customer information; (2) preventing unwarranted access and use of customer information; and (3) insuring the security and confidentiality of customer records.

We would urge the Commission to require financial institutions to implement an information security program which meets the statutory requirements while granting financial institutions the ability to make the appropriate determinations with respect to how best to achieve those requirements. Given the wide range of financial institutions that will be

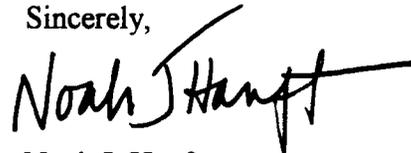
subject to the Commission's Safeguards, it would be difficult to develop effective Safeguards that did not allow for such flexibility.

For example, the Safeguards should allow each financial institution to assess the risks which may threaten its customer information systems. It should also allow financial institutions to weigh the sensitivity of information and the threats to the information systems. The financial institution should be responsible for assessing what types of risk controls should be utilized and for adjusting its risk assessment in light of technology. Although the Commission may wish to include some specific factors which should be considered by each financial institution when complying with the Safeguards, the responsibility should fall on the financial institution's management to determine the appropriate procedures in order to comply with the objectives of the Safeguards.

* * * * *

Once again, MasterCard commends the Commission for requesting comment prior to issuing the Safeguards, and we greatly appreciate the opportunity to provide our comments. If you have any questions concerning our comments, or if we may otherwise be of assistance in connection with this issue, please do not hesitate to call me, at the number indicated above, or Michael F. McEneney at Sidley & Austin, at (202) 736-8368, our counsel in connection with this matter.

Sincerely,



Noah J. Hanft

cc: Joshua Peirez (MasterCard International)
Michael F. McEneney (Sidley & Austin)