

Joshua L. Peirez
Vice President &
Legislative/Regulatory Counsel

MasterCard International

Law Department
2000 Purchase Street
Purchase, NY 10577-2509

914 249-5903
Fax 914 249-4261
E-mail joshua_peirez@mastercard.com
Internet Home Page:
<http://www.mastercard.com>

*MasterCard
International*



Via Hand Delivery

October 9, 2001

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 Sir:

This comment letter is filed on behalf of MasterCard International Incorporated ("MasterCard")¹ in response to the proposed rule ("Proposal") published by the Federal Trade Commission (the "Commission") to implement standards for safeguarding customer information pursuant to sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act ("GLB Act"). MasterCard appreciates this opportunity to comment on this important matter.

At the outset, MasterCard wishes to commend the Commission for its efforts to "create a general procedural framework" which is intended to be flexible and to allow each information security program to be crafted appropriately based on the size and complexity of the particular financial institution. The objectives of establishing a general framework and providing flexibility for financial institutions are important ones, and we urge that the Commission continue to use them as guideposts in developing the final rule. We also offer the following more specific comments for consideration by the Commission when preparing its final rule.

§314.1 Purpose and Scope

The Proposal and Supplementary Information suggest that the Proposal is intended to cover information about "customers" and not information about "consumers" or other entities. MasterCard believes that it is important to

¹ MasterCard is a global membership organization comprised of financial institutions that are licensed to use the MasterCard service marks in connection with a variety of payments systems.

limit the scope of the Proposal to "customer" information in order to implement Congress' intent in enacting the GLB Act. Congress' intent is clearly evident from the plain language of section 501(b) of the GLB Act which 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 noted the significance of the distinction between the two terms when the Commission adopted its rule implementing the privacy provisions of the GLB Act ("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 to the Privacy Rule 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.

The scope of the Proposal, however, does not implement this distinction and appears to be inconsistent with the language and intent of the GLB Act. Specifically, section 314.1(b) of the Proposal states that the Proposal "applies to all customer information in your possession, regardless of whether such information pertains to individuals with whom you have a customer relationship, or pertains to the customers of other financial institutions that have provided such information to you." Although the Proposal states that its definition of "customer" is the same as the definition of that term found in the Privacy Rule, the Proposal actually uses the definition far more expansively. Under the Privacy Rule, the question of whether an individual is a customer of a financial institution turns entirely upon that individual's relationship with that financial institution. Specifically, an individual is a "customer" of a financial institution only if the financial institution has a "continuing relationship" with the individual under which it provides financial products or services for consumer purposes. If an individual obtains financial products or services from a financial institution but does not have a continuing relationship, that individual is a "consumer" of the financial institution, not its customer. For example, under the Privacy Rule, if financial institution A shares its customer list with financial institution B pursuant to notice and opt out, or under an exception to the notice and opt out requirements, the individuals on that list do not become the "customers" of financial institution B and the portions of the Privacy Rule regarding customers do not apply to financial institution B with respect to those individuals (unless financial institution B establishes its own customer relationship with the individuals). Under the Proposal, however, financial institution B would effectively be forced to treat every one of those individuals as a

"customer" even if financial institution B never establishes a "continuing relationship" or any other relationship with those individuals. As a result, the approach set forth in the Proposal does not reflect the distinction between a "customer" and a "consumer" in this context and effectively would force a financial institution to treat all information about individuals as customer information if those individuals might be customers of another financial institution.

As a result, we are concerned that the scope provision of the Proposal will not provide sufficient guidance to enable financial institutions to efficiently and effectively determine which information is covered by the Proposal and which information is not. This problem will be particularly acute for many of the financial institutions within the Commission's jurisdiction who have diversified operations and for smaller entities who are deemed to be "financial institutions" for the first time under the GLB Act. For example, the Proposal provides little guidance for small businesses to determine whether information they may have from various sources must be handled under the Proposal if those businesses become financial institutions under the GLB Act.

To address these issues, we strongly urge the Commission to modify the scope of the Proposal to provide certainty regarding the types of information covered by the Proposal and the types of information which are not. We believe that the scope can be appropriately drawn by simply utilizing the approach set forth by the banking agencies in their information safeguard guidelines. Specifically, we urge that section 314.1(b) be revised to read as follows:

(b) Scope. This rule applies to customer information maintained by or on behalf of a financial institution over which the Federal Trade Commission ("FTC" or "Commission") has jurisdiction. This rule refers to such entities as "you."

We also urge the Commission to consider allowing a financial institution within its jurisdiction to be deemed in compliance with the Commission's final rule if the institution is in compliance with the corresponding guidelines issued by the banking agencies or other agencies. In this regard, there may be many financial institutions that are members of larger corporate families which are subject predominantly to the jurisdiction of the banking agencies. Although distinctions between the banking agencies' guidelines and the Commission's final rule may be minor, it would serve no purpose for a diversified financial corporation with an overall corporate security program in place, for example, to have to make minor changes in its program in order for one of its financial institutions to comply, solely in a technical sense, with the Commission's final rule.

§314.2 Definitions

Section 314.2(a) of the Proposal states that “[e]xcept as modified by this rule or unless the context otherwise requires, the terms used in this rule have the same meaning as set forth in the Commission’s [Privacy Rule].” The Supplementary Information to the Proposal states by way of example, that the terms “customer” and “affiliate” have the same meaning as set forth in the Privacy Rule. We believe that this approach accurately reflects Congress’ intent, and we urge that it be embodied in the final rule. In view of the potential confusion created by the scope provisions as discussed above, however, and given the significance of the definition of “customer” with respect to interpreting the requirements of the Proposal, we urge that the Commission specifically include the appropriate definition of the term “customer” in the final rule itself. Specifically, we urge that the final rule include the following definition:

“(b) ‘Customer’ means any customer of yours as defined in 16 C.F.R. 313.3(h).”

Section 314.2(b) of the Proposal states that “customer information” “means any record containing nonpublic personal information, as defined in 16 CFR 313.3(n), about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.” This definition is extremely broad, and we are concerned that it could actually undermine the effectiveness of the Proposal. In this regard, it is important that financial institutions be able to readily identify the types of information covered by the Proposal so that they may design appropriate safeguards to protect it. For the reasons discussed above, however, the proposed definition of customer information would make it extremely difficult for a financial institution to distinguish which information in its files is covered by the Proposal and which is not.

To address this issue, it is important that the definition of “customer information,” like the definition of customer, 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 Proposal 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, as discussed above, 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 Proposal than they do under corresponding provisions of the Privacy Rule.

The definition of “customer information” also expands the Proposal to cover information maintained by an affiliate of a financial institution even if that

affiliate is not itself a financial institution. We believe that this approach is inconsistent with the requirements of the GLB Act which imposes safeguarding obligations only on "financial institutions." Moreover, we believe that such an expansion is unnecessary. In this regard, the standard and "elements" set forth in sections 314.3 and 314.4 of the Proposal should be adequate to address this issue. Those provisions require a financial institution to establish procedures to safeguard the financial institution's customer information, and we believe that those provisions would cover information when a financial institution chooses to store the information with another party. Thus, there is no need to expand the definition of "customer information" to expressly cover that information. In addition, such an expansion only creates confusion regarding the actual scope of the Proposal. In particular, that portion of the definition of customer information raises questions whether any information "about a customer of a financial institution" would be covered by the definition if that information is maintained by an "affiliate" of any financial institution. There is no suggestion in the legislative history to the GLB Act that the safeguard requirements of section 501 or 505(b)(2) should be cast so broadly.

In order to address these issues, we urge the Commission to adopt the approach used by the banking agencies in promulgating their safeguarding standards. Specifically, we urge that the Commission adopt the following definition of customer information:

"'Customer information' means any record containing nonpublic personal information, as defined in 16 C.F.R. 313.3(n) about your customer, whether in paper, electronic, or other form, that is maintained by you or on your behalf."

Consistent with the definition of "customer," we would also urge the Commission to expressly state that the Proposal covers only 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 expressly stating in the final rule that it applies only to "customers" who obtain financial products or services for "personal, family, or household purposes."

§ 314.3 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 a fundamental and guiding principle of the final rule. For example, the final rule should provide several general options with respect to achieving a satisfactory level of security. If the final rule becomes 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.

We also commend the Commission for acknowledging that a financial institution's safeguards need only be "reasonably designed to achieve the objectives" of the final rule. This clarification is critical since even the most conscientious financial institution could not meet a standard which required financial institutions to achieve the objectives in all possible circumstances. We urge the Commission to maintain this standard in the final rule.

The Proposal states, however, that one of the objectives in establishing a security program shall be to "[i]nsure the security and confidentiality of customer information." This language appears to be intended to implement section 501(b)(1) of the GLB Act which directs the Commission to establish appropriate standards for financial institutions "to insure the security and confidentiality of customer records and information." We are concerned that use of the word "insure" suggests that the Commission intends to set a higher standard than is likely intended. Specifically, a financial institution's safeguards must be "reasonably designed" to meet the objectives of the final rule, but one objective suggests that the financial institution must "insure" compliance in all cases. Therefore, we request the Commission use the word "protect" rather than "insure." This would be consistent with the Commission's intent without creating ambiguity as to what is expected of financial institutions.

§ 314.4 Elements

The Supplementary Information indicates that the Commission has provided a "framework" for developing the required safeguards, but that the Proposal "leave[s] each financial institution discretion to tailor its information security program to its own circumstances." Again, we commend the Commission for its commitment to providing flexibility to financial institutions and urge the inclusion of this clarification in the Supplementary Information to the final rule.

The Proposal would require a financial institution to designate an employee or employees to coordinate the information security program. We believe the Commission has taken the correct approach by allowing the financial institution to determine which employee is in the best position to develop and implement the program. In this regard, there will be accountability within the

financial institution while allowing the institution to designate the most appropriate individual to act as the "point person" on its information security safeguards.

The Proposal would also require financial institutions to identify "reasonably foreseeable" security risks. We believe this is the appropriate standard and it should be retained in the final rule. We also believe it appropriate for the Commission to indicate certain broad areas that a financial institution should consider without mandating that each financial institution necessarily adopt specific protections in every broad area. In this regard, the Proposal remains consistent with the overall theme that each financial institution should adopt safeguards that are appropriate with respect to that financial institution's particular needs.

A financial institution would be expected to "regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures." We applaud the Commission for not suggesting that financial institutions must have such tests performed by particular individuals, such as independent third parties. Although the banking agencies included such guidance with respect to the use of independent third parties, we believe the final rule should allow each financial institution the flexibility to conduct its tests in the manner deemed most appropriate by that financial institution.

The Proposal requires financial institutions to select and retain service providers that are "capable of maintaining appropriate safeguards for the customer information at issue." We believe the Commission has chosen an appropriate standard for financial institutions when selecting their outside service providers. The Proposal is preferable to other alternatives which require financial institutions to conduct "due diligence" when selecting service providers.

We also commend the Commission for its requirement that a financial institution select providers that are capable of maintaining "appropriate" safeguards, without prescribing what may be considered "appropriate." In this regard, the Commission has provided financial institutions the flexibility to make such determinations on a case-by-case basis depending on the unique circumstances of each relationship and the nature of information to be provided to the service provider. For this reason, this language should be maintained in the final rule.

We also applaud the Commission for requiring service providers to implement the appropriate safeguards by contract, but not requiring financial institutions to monitor or audit its service providers. Such a requirement could prove extremely burdensome, especially to smaller financial institutions. However, by requiring service providers to be contractually bound to maintain the appropriate safeguards, the Commission has ensured that financial institutions will have the ability to take appropriate action if a service provider does not meet its obligation.

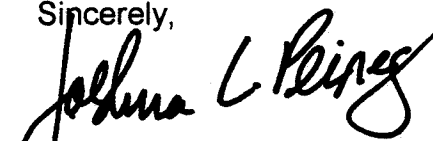
§ 314.5 Effective Date

The Proposal provides that a financial institution must implement an information security program pursuant to the final rule within one year from the date on which a final rule is issued. We believe that this will provide sufficient time for financial institutions to review the final rule and implement an information security program. However, we are concerned that the Commission has not provided a grandfather period for agreements with service providers. For example, the banking agencies provided a two-year period in which a contract between a financial institution and its service provider need not meet the requirements of the guidelines if the contract was entered into prior to approximately five weeks after the final rule was issued. This grandfather period is necessary in light of the fact that not all existing contracts with service providers may comply with the final rule. The Commission has specifically requested comment on this issue and we urge the Commission to adopt a grandfather period similar to that included in the banking agencies' information safeguarding guidelines.

* * * * *

Once again, MasterCard appreciates the opportunity to comment on this important matter. 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 Brown & Wood, at (202) 736-8368, our counsel in connection with this matter.

Sincerely,



Joshua L. Peirez
Vice President &
Legislative/Regulatory Counsel

cc: Michael F. McEneney, Esq.