Jodi Golinsky
Vice President
Legislative/Regulatory & Privacy Counsel

MasterCard International
Law Department
2000 Purchase Street
Purchase, NY 10577-2509
914 249-5978
Fax 914 249-3648
E-mail jodi_golinsky@mastercard.com
www.mastercard.com

16

MasterCard International

Via Electronic Delivery

March 29, 2004

Public Information Room
Office of the Comptroller of the Currency
250 E Street, SW, Mail Stop 1-5
Washington, DC 20219
Attention: Docket No. 03-27

regs.comments@occ.treas.gov

Regulation Comments
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, NW
Washington, DC 20552
Attention: No. 2003-62

regs.comments@ots.treas.gov

Ms. Jennifer J. Johnson
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551

regs.comments@federalreserve.gov

Mr. Robert E. Feldman
Executive Secretary
Attention: Comments/Executive Secretary Section
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429

comments@fdic.gov

Ms. Becky Baker
Secretary of the Board
National Credit Union Administration
1775 Duke Street
Alexandria, VA 22314-3428

regcomments@ncua.gov

Federal Trade Commission
Office of the Secretary, Room 159-H
600 Pennsylvania Avenue, NW
Washington, DC 20580
Attn: Project No.P034815

GLBnotices@ftc.gov

Ms. Jean A. Webb
Secretary
Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street, NW
Washington, DC 20581

secretary@cftc.gov

Mr. Jonathan G. Katz
Secretary
Securities and Exchange Commission
450 5th Street, NW
Washington, DC 20549-0609
Attn: File No. S7-30-03

rule-comments@sec.gov

Re: Alternative Forms of Privacy Notices

To Whom It May Concern:

MasterCard International Incorporated ("MasterCard")[1] submits this comment letter in response to the Interagency Proposal (the "Proposal") to Consider Alternative Forms of Privacy Notices Under the Gramm-Leach-Bliley Act (the "GLBA") issued by the Office of the Comptroller of the Currency, Office of Thrift Supervision, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Federal Trade Commission, Commodity Futures Trading Commission, and Securities and Exchange Commission (the "Agencies"). We commend the Agencies for their efforts to simplify the privacy notices required under the GLBA, and we appreciate the opportunity to provide our comments regarding the Proposal.

MasterCard strongly supports the Agencies' objective of providing consumers GLBA privacy notices that are more simple, concise, and easy to understand and compare. We believe that permitting such simple notices in lieu of the more detailed

[1] MasterCard is a SEC-registered private share corporation that licenses financial institutions to use the MasterCard service marks in connection with a variety of payments systems.

notices required under the Agencies existing GLBA regulations (the "Existing Rule") would be well within the scope of the Agencies' GLBA rulemaking authority. We are concerned, however, that unless the privacy notices required at the federal level are established as the uniform national standard, the objective of establishing simple privacy notices will not be achieved. In this regard, a number of states have already enacted privacy statutes requiring disclosures that, at a minimum, would lengthen and complicate any simplified notice developed by the Agencies. Many other states are considering similar legislation. Unless these state laws are preempted they will significantly undermine, if not entirely eliminate, many of the benefits the Agencies seek to provide through simplified notices. Accordingly, we urge the Agencies to pursue legislative and other solutions to create a uniform national standard for the GLBA notices that are the subject of the Proposal. If combined with federal preemption, we believe that a single, short form notice approach could be adopted in a manner that fully satisfies the statutory requirements of the GLBA and produces substantial improvements in the GLBA notices. The following sets forth more specific comments regarding the Proposal.

Goals of the Privacy Notice

In our view, the goal of any revised GLBA privacy notice requirements should be to convey key information to consumers about a financial institution's information practices in a manner that is likely to be meaningful to consumers and easy to understand. To achieve this goal, the notice must be brief, and must convey the required elements using concepts that consumers are likely to be able to comprehend without the need for independent knowledge of industry practice or detailed explanation. In essence, the notice should convey information at a basic conceptual level to which consumers can relate. Appendices A and B to the Proposal appear to point in the right direction by using categories that consumers are likely to understand without additional information (*e.g.* categorizing information based on source, and third parties based on use of the information). Another key goal of the privacy notice is to convey the information required by the GLBA in a single notice, without the need for both a long and short form notice. The following describes how these goals can be achieved.

Elements and Language of the Privacy Notice

We believe that the language of the GLBA fully supports the type of short notice the Agencies are considering. The core privacy notice requirements of the GLBA are set forth in Section 503. *See* 15 U.S.C. § 6803. Section 503(a) provides that a financial institution must furnish an initial and annual notice "of such financial institution's policies and practices with respect to --

> (1) disclosing nonpublic personal information to affiliates and nonaffiliated third parties, consistent with Section 502, including the categories of information that may be disclosed;
>
> (2) disclosing nonpublic personal information of persons who have ceased to be customers of the financial institution; and

(3) protecting the nonpublic personal information of consumers."

15 U.S.C. § 6803(a).

Section 503(b) provides more specific instructions from Congress regarding what must be included in the notices required under Section 503(a). Specifically, Section 503(b) states that the initial and annual disclosures "*shall* include" four basic elements: (i) the categories of nonpublic personal information that are collected by the financial institution; (ii) the policies and practices of the institution with respect to disclosing nonpublic personal information to nonaffiliated third parties; (iii) the policies that the institution maintains to protect the confidentiality and security of nonpublic personal information in accordance with Section 501; and (iv) the disclosures required, if any, under Section 603(b)(2)(A)(iii) of the Fair Credit Reporting Act. 15 U.S.C. § 6803(b). (Emphasis added.)

Section 503 sets forth the only basic information that the initial and annual GLBA privacy notices must contain. A fifth notice element -- the opt-out requirement -- is triggered only if the financial institution wishes to disclose nonpublic personal information to nonaffiliated third parties in certain circumstances. More specifically, Section 502 of the GLBA requires a financial institution to include in its initial and annual notices a disclosure of the consumer's right to opt out of certain types of disclosures of information to nonaffiliated third parties. *See* 15 U.S.C. § 6802(a) and (b)(l). A sixth and final notice component is required if the financial institution provides nonpublic personal information to nonaffiliated third parties "to perform services for or functions on behalf of the financial institution." If the financial institution makes such disclosures, it must disclose that fact in its initial and annual notices. 15 U.S.C. § 6802(b)(2).

Beyond these basic elements, there is nothing that *must* be included in the initial and annual GLBA notices. Moreover, Congress granted to the Agencies the authority to interpret and implement these notice requirements. Specifically, Section 503(a) makes it clear that "[s]uch disclosures shall be made in accordance with the regulations prescribed [by the Agencies] under Section 504." *Id.* Section 504 grants the Agencies authority to adopt "such regulations as may be necessary to carry out the purposes of [the GLBA privacy provisions] with respect to the financial institutions [within their respective jurisdictions]." 15 U.S.C. § 6804(a)(1). The following discusses each of those disclosure elements in the context of a short form notice.

1. <u>Categories of Nonpublic Personal Information Collected</u>

Section 503(b) makes it clear that the GLBA privacy notices must include a disclosure regarding the "categories of nonpublic personal information that are collected by the financial institution." The conceptual approach taken by the Agencies in the Existing Rule already provides a helpful framework for defining the "categories" of nonpublic personal information collected. In particular, the Existing Rule sets forth the following examples for categorizing information collected: (i) information from the

consumer; (ii) information about the consumer's transactions with the financial institution or its affiliates; (iii) information about the consumer's transactions with nonaffiliated third parties; and (iv) information from a consumer reporting agency. We believe that these four categories cover the bulk of information financial institutions collect about consumers and should form the basis for new disclosures regarding information collected. By building on the approach used in Appendices A and B, these categories of information can be succinctly described in a privacy notice using language such as the following:

We may collect information about you from:

- **your account or other financial relationships, including your transactions and payment history, with us, our affiliates, or others**
- **applications or other information you provide to us**
- **credit reports we obtain about you.**

These three categories of information could be disclosed with a box or line on which the financial institution could indicate "yes" for each category the financial institution collects and indicate "no" for each category it does not. In addition, we would recommend that a fourth category be made available for those financial institutions that collect information not covered by the first three categories. Specifically, a financial institution that collects information not covered by the first three categories should be able to indicate that it collects information from "other sources" (*e.g.* as set forth in Appendix B).

Describing the categories in these ways serves two important functions. First, these disclosures can be made clearly and simply and therefore can be presented in a way a consumer is more likely to read and understand. Second, by describing the information in a context consumers can relate to without independent knowledge of detailed information about information practices, the disclosures make the categories readily understandable. For example, a consumer can fairly easily understand what information is encompassed in his or her transactions and payment history with the financial institution, its affiliates, and others. Consumers have frequent experience, including through billing statements and other information disclosed to them, that makes this disclosure easy to understand. Similarly, consumers are aware of what information they provide to financial institutions and there appears to be a broad awareness of the kinds of information in credit reports. As a result, using these simple disclosures about the categories of information collected would enable consumers to understand the significance and nature of the information that is covered by the disclosure in a form that is easy to read.

2. **Categories of Nonaffiliated Third Parties To Whom Information is Disclosed**

Section 503(b) mandates that the privacy notices must include the categories of nonaffiliated third parties to which nonpublic personal information will be disclosed by a financial institution. We believe that, in order to make this disclosure useful to consumers, the term "categories" should be defined in a manner that has meaning to consumers. In our view, the best approach to achieving this is to build on the conceptual approach used in defining the categories of information collected. Specifically, the categories of nonaffiliated third parties should be defined in a manner to which consumers can relate based on their own experiences and without a broad or deep understanding of industry practice. One approach for achieving this is embodied in Appendices A and B, which essentially define the categories of third parties based on what those parties do with the information. For example, Appendix A divides the third parties into those that use the information for the following purposes: (i) to offer their products and services to consumers; (ii) to perform services including joint marketing services; and (iii) in accordance with the exceptions provided in the GLBA. These categorizations based on functionality increase the likelihood that consumers will understand the significance of the respective disclosures made to the organizations included in those categories.

In particular, most consumers can readily identify with receiving solicitations from third parties and can make a judgment with respect to that practice based on its significance to them. Experience with the GLBA notices required under the Existing Rule, however, suggest that disclosures regarding service provider arrangements are less likely to be meaningful to consumers. In fact, this disclosure which has been required in response to the provisions of Section 502(b)(2) of the GLBA, may actually create more confusion than clarity regarding a financial institution's information practices. As the Agencies examine ways to make the GLBA privacy notices more effective, it would be helpful if the Agencies would consider limiting the circumstances under which this disclosure must be provided. For example, it would be helpful if the Agencies were to examine whether this particular disclosure requirement could be narrowed under the Agencies' authority to grant exceptions under Section 504(b) of the GLBA. In any event, in those circumstances where the disclosure is required, we urge the Agencies to make the disclosure as simple as possible. Appendices A and B include examples which may be helpful in this regard.

A similar issue arises in the context of privacy notice provisions covering disclosures made to third parties under these so-called "as permitted by law" exceptions. Notice provisions regarding these types of disclosures appear to provide little, if any, utility to consumers. In addition, because of the diversity of the exceptions it is difficult to include in a privacy notice a brief description that explains these exceptions in a meaningful way. To address this issue, we urge that the Agencies consider whether information practices with respect to the "as permitted by law" exceptions can be eliminated entirely from the GLBA privacy notices. The language of Section 502(e) which makes clear that the notice and opt-out provisions of Sections 502(a) and (b) do not apply

to the exceptions may provide a basis for the Agencies to determine that these disclosures need not be included in the GLBA notices.

3. Information Safeguard Policies

Section 503(b) mandates that the GLBA privacy notices must include a disclosure regarding the policies a financial institution "maintains to protect the confidentiality and security" of nonpublic personal information. We believe that the short, concise disclosure approach already embodied in the Existing Rule achieves the objectives of the statute and can easily be adapted to a short-form notice.

4. FCRA Affiliate Sharing Disclosure

Section 503(b) makes clear that a financial institution must include in its GLBA privacy notice the FCRA affiliate sharing disclosure "if any" is required under the FCRA. Through the Existing Rule, this provision has been interpreted to require a financial institution to include the FCRA affiliate sharing notice in its initial and annual GLBA notices if the financial institution shares information among its affiliates in a manner covered by the FCRA.

Combining the affiliate sharing notice with the GLBA notices presents significant challenges. The biggest challenge arises from the fact that the GLBA and FCRA are very different in terms of the types of information they regulate. The GLBA regulates nonpublic personal information which the Agencies have interpreted to include all "personally identifiable financial information." The FCRA, on the other hand, regulates any information that is a "consumer report," a term that is given meaning through a highly complex definition that is subject to exceptions that have no meaning in the context of the GLBA. As a result, any requirement that the GLBA notices include the FCRA affiliate sharing provisions magnifies the complexity of the disclosures in significant ways. Appendix A and Appendix B to the Proposal highlight this point. For example, the affiliate sharing disclosures included in those two formats are the longest and most detailed disclosures in the samples. The affiliate sharing disclosures also, by necessity, depart from the simple information categories the Agencies established under the Existing Rule and describe subsets of the information collected in ways that have meaning under the FCRA but have the potential to create confusion when included in a disclosure designed to deal with a much different scope and focus based on the definition of "nonpublic personal information."

We believe that the Agencies have the authority to address this problem. As noted above, Section 503(b) states that the initial and annual GLBA notices must include the FCRA affiliate sharing notices "if any" are required under the FCRA. 15 U.S.C. § 6803(b)(4). The FCRA itself only requires that the affiliate sharing notice be given once to each consumer covered by the particular affiliate sharing practices. As a result, the language in Section 503(b) with respect to affiliate sharing appears to require that the GLBA notice include the FCRA affiliate sharing language only if the consumer to whom the GLBA notice is provided has not otherwise received the FCRA notice. If the

Agencies were to adopt this interpretation as part of their efforts to revise the GLBA notice requirements, financial institutions would, at a minimum, have the flexibility to simplify the GLBA notices in meaningful ways. For example, under such an interpretation, a financial institution could eliminate the FCRA notice and opt-out provisions from the GLBA notices for any consumer that already had received the financial institution's FCRA affiliate sharing notice. Of course, the GLBA notice would continue to include the fact that information covered by the notice is shared with affiliates (as applicable) but would not need to include the FCRA affiliate sharing notice and opt-out itself.

5. Opt Out for Disclosures to Nonaffiliated Third Parties

In our view, the methods provided to consumers for opting out of disclosures to nonaffiliated third parties should be easy to use and understand. We believe that Appendices A and B include workable examples that might be used for these purposes. In addition, we believe it is important that financial institutions have flexibility to give consumers an array of choices with respect to the practices from which consumers wish to opt out. For example, financial institutions should be permitted to allow consumers to make their opt-out selections based on different factors including different types of nonaffiliated third parties to whom the information is transmitted, different types of information, and different types of product offers. Such choices should be permissible so long as the consumer has the right to opt out of all of the disclosures made to nonaffiliated third parties covered by Section 502(b).

6. Information Provided to Nonaffiliated Service Providers

This item is covered in #2 above.

Other Issues

In making any revisions to the Existing Rule, we believe it would be important for the Agencies to provide model language or disclosures that may be used in the GLBA notices. In addition, we urge the Agencies to make it clear that use of the model language or disclosures will be deemed to comply with the GLBA. It also would be important for a financial institution to have the flexibility to present its GLBA privacy notice using different language or formats and to provide additional privacy information with the notice, so long as the financial institution is complying with the revised requirements. Such an approach is consistent with the approach taken by the Agencies under the Existing Rule, and we believe it should be retained.

Conclusion

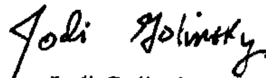
In sum, we believe that the GLBA privacy notice provisions can be implemented through a single, short form disclosure that covers all of the statutorily required issues in a manner that is meaningful to consumers. We believe this result can only be achieved, however, if the GLBA notices are given preemptive effect. We therefore urge that the Agencies not adopt any new GLBA disclosure requirements unless they are

accompanied by federal preemption. In particular, financial institutions should not be required to revise their existing privacy policies to accommodate changes at the federal level only to continue to have to update and revise the policies based on changes at the state level. Under such circumstances, any revisions made to accommodate the GLBA requirements would be largely wasted efforts because the goal of simplification cannot be met so long as state law requirements continue to impede uniformity.

* * * * *

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 LLP, at (202) 736-8368, our counsel in connection with this matter.

Sincerely,



Jodi Golinsky
Vice President
Legislative/Regulatory & Privacy Counsel

cc: Michael F. McEneney, Esq.