RUSSELL W. SCHRADER
Senior Vice President and
Assistant General Counsel

October 9, 2001

By Electronic Delivery and Hand Delivery

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

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

Dear Sir or Madam:

This comment letter is submitted on behalf of Visa U.S.A. Inc. ("Visa") in response to the Notice of Proposed Rulemaking issued by the Federal Trade Commission ("FTC") to implement Section 501 of the Gramm-Leach-Bliley Act ("GLB Act"). We appreciate the opportunity to comment on this important matter. In doing so, Visa provides comment generally on the proposed Safeguards Rule (the "Rule"), as well as on several specific provisions.

The Visa payments system is a membership organization comprised of 21,000 financial institutions licensed to use the Visa servicemarks. It is the largest consumer payment system in the world. Over 1 billion Visa-branded cards are accepted at over 20 million locations. Consumers use them to buy over $1.8 trillion in goods and services annually on a worldwide basis. Visa U.S.A., which is part of the Visa payments system, is comprised of 14,000 U.S. financial institutions. U.S. customers carry about 350 million Visa-branded cards and use them to buy over $900 billion worth of goods and services annually.

GENERAL COMMENTS ON THE PROPOSED RULE

As a general matter, Visa commends the FTC for proposing a Rule that is consistent with the approach set forth in the federal banking agencies' final guidelines ("Banking Agency Guidelines"), which establish a framework focusing on the "process" that financial institutions should follow in designing and implementing an information

VISA U.S.A. INC.
Post Office Box 194607
San Francisco, CA 94119-4607
U.S.A.
Phone 415 932 2178
Fax 415 932 2525

security program, without attempting to specify in detail how a financial institution should structure its information security program, or the particular safeguards to be employed in its security program.[1] This "general framework" approach meets the FTC's obligation to implement the standards prescribed under Section 501(b) of the GLB Act and provides appropriate guidance to financial institutions, without curtailing the flexibility of financial institutions in developing and implementing an information security program that best fits their particular needs.

FTC SECURITY STANDARDS SHOULD BE CONSISTENT WITH BANKING AGENCY GUIDELINES, BUT SHOULD PROVIDE ADDITIONAL FLEXIBILITY WHERE NEEDED

Visa also commends the FTC for providing additional flexibility to financial institutions under its jurisdiction in designing and implementing information security programs, while simultaneously striving to ensure that the FTC's Rule is consistent with the Banking Agency Guidelines. The FTC and the federal banking agencies provided consistent final privacy rules, and it is essential that the same approach be taken in addressing security standards. Inconsistent rules would be particularly burdensome for entities that have some affiliates subject to the FTC's Rule and other affiliates subject to the Banking Agency Guidelines.

Nonetheless, Visa commends the FTC for providing additional flexibility in its Rule to financial institutions under its jurisdiction in order to accommodate for the differences between institutions under FTC jurisdiction and those regulated by the federal banking agencies. For example, the FTC's proposed Rule requires a financial institution subject to the Rule to designate an employee or employees to coordinate the institution's information security program in order to ensure accountability within each entity for achieving adequate safeguards. The Banking Agency Guidelines, in contrast, require financial institutions to involve and report to their boards of directors. Visa commends the FTC for the additional flexibility in this area because, as pointed out by the FTC in the supplemental information to the proposed Rule, many entities subject to the FTC's jurisdiction are not controlled by boards of directors. Visa also notes with approval the additional flexibility provided by the FTC with respect to managing and controlling risk and testing.

[1] On February 1, 2001, the Office of the Comptroller of the Currency, Federal Reserve Board, Federal Deposit Insurance Corporation and Office of Thrift Supervision issued final Guidelines to implement Section 501 of the GLB Act.

THE FTC SECURITY STANDARDS SHOULD ONLY DIRECTLY APPLY TO A FINANCIAL INSTITUTION'S HANDLING OF INFORMATION ABOUT ITS OWN CUSTOMERS

The FTC's proposed Rule appears to apply directly to all customer information in the possession of a financial institution over which the FTC has jurisdiction, regardless of whether such information pertains to individuals with whom that institution has a customer relationship, or pertains to information maintained by the institution regarding the customers of other financial institutions for which, for example, the institution is providing services. The FTC Rule differs from the Banking Agency Guidelines, which apply directly to information in the possession of a financial institution only if that information pertains to individuals with whom that institution has a customer relationship.

Visa strongly urges the FTC to revise its Rule to conform to the Banking Agency Guidelines and thus, provide that the Rule only establishes safeguards for a financial institution's handling of information about its own customers. Section 501(a) of the GLB Act clearly provides that the security requirements only apply to a financial institution's handling of information about its own customers. More specifically, Section 501(a) states that "[i]t is the policy of the Congress that each financial institution has the affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." Section 501(a) clearly expresses Congress' intent that a financial institution is obligated by statute only to protect the security and confidentiality of nonpublic personal information of its own customers; Congress did not intend these obligations to extend directly to information that the financial institution might possess about the customers of other financial institutions or customers of nonfinancial institutions.

In addition, broadening the scope of Section 501(a) of the GLB Act is unnecessary because the broadened scope would apply to many entities already required to adopt security standards due to contractual provisions in their agreements with the financial institutions that entrust them with customer information for servicing and other purposes. Financial institutions subject to FTC jurisdiction that provide services to other financial institutions regulated by the federal banking agencies already must comply with contract requirements set forth in the Banking Agency Guidelines. In addition, financial institutions subject to FTC jurisdiction are subject to regulation and examination by the federal banking agencies under the Bank Service Company Act when providing services to other financial institutions that are regulated by the federal banking agencies. Moreover, financial institutions subject to FTC jurisdiction that provide services to financial institutions subject to FTC jurisdiction already must comply with contract requirements set forth in the FTC's Rule.

With respect to other entities that are not already required to adopt security standards, the costs of regulating these entities outweigh the benefits. The broad scope of the Rule would sweep in thousands of financial institutions subject to FTC jurisdiction that receive customer information from financial institutions, but are not service providers to those institutions. At the same time, the Rule would omit thousands of other entities that receive information from nonaffiliated financial institutions, but are not covered by the FTC's Rule because the entities are not financial institutions. Therefore, the benefits of the broadened scope will be uneven and unpredictable. At the same time, financial institutions that are swept up by the broadened scope of the Rule will incur huge expenses to develop and implement the required security programs. To avoid this, the FTC should revise the Rule to specify application only to a financial institution's handling of information about its own customers.

Visa strongly urges that even if the FTC determines not to limit the Rule's scope to include only a financial institution's handling of its own customer information, that the Rule be revised not to apply to financial institutions under the jurisdiction of the FTC to the extent that the institutions are acting as service providers or subservicers to financial institutions that are subject to the Banking Agency Guidelines. Applying the FTC's final Rule to these financial institutions would not provide any additional benefits for customers and would be burdensome to these institutions. Such financial institutions already are subject to contractual obligations under the Banking Agency Guidelines. In particular, the Banking Agency Guidelines provide that financial institutions subject to the banking agencies' jurisdiction must require their service providers by contract to implement appropriate security measures designed to meet the objectives of the Banking Agency Guidelines. These contract provision requirements with service providers took effect on July 1, 2001, unless the contract is grandfathered under the Guidelines (that is, a contract with a service provider dated on or before March 5, 2001 would have July 1, 2003 as a compliance deadline). The Banking Agency Guidelines also provide that where indicated by its risk assessment, a financial institution must monitor a service provider to confirm that the service provider is in fact employing the service provider's security measures.

In addition, under the Bank Service Company Act, financial institutions and other entities that provide services to banks and other institutions that are covered by the Banking Agency Guidelines are subject to regulation and examination by the federal banking agencies. In particular, the Bank Service Company Act, in relevant part, provides that whenever a bank that is subject to examination by an appropriate federal banking agency (or any subsidiary or affiliate of such a bank that is subject to examination by that agency) outsources its banking activities to a service provider, the performance of such activities by the service provider is subject to regulation and examination by such agency to the same extent as if such services were being performed by the bank itself on its own premises. Thus, the appropriate federal banking agency may examine the service provider with respect to its performance of activities on behalf of the bank, including on issues relating to security. In addition, the bank must notify

the appropriate federal banking agency of the existence of the service relationship within 30 days after the making of such service contract or the performance of the service, whichever occurs first.

Thus, financial institutions subject to the banking agencies' jurisdiction already must require their service providers by contract to implement appropriate security measures designed to meet the objectives of the Banking Agency Guidelines. In addition, where appropriately based on their risk assessment, these financial institutions must monitor their service providers' compliance with the security measures required by the contractual requirements. As a result, federal banking agencies already have the authority to examine entities that provide services to banks or other financial institutions under the agencies' jurisdictions, including on issues relating to security. These requirements adequately ensure that financial institutions that are acting as service providers to banks, or other financial institutions subject to the Banking Agency Guidelines, are protecting customer information received from those institutions. Requiring such service providers also to comply with the FTC's Rule would not provide any additional protections for customers, but nevertheless could impose additional burdens on such service providers. Although the FTC's proposed Rule is similar to the Banking Agency Guidelines, some differences do exist and still other differences could develop in the future. Requiring these service providers to keep informed of the formal and informal interpretations that might be given to the FTC's Rule in the future would place regulatory burdens on such service providers without any purported corresponding benefits to customers. Thus, at a minimum, the FTC should revise the scope of its Rule to provide that the Rule does not apply to financial institutions under the jurisdiction of the FTC to the extent that the institutions are acting as service providers or subservicers to financial institutions that are subject to the Banking Agency Guidelines.

GRANDFATHERING PROVISION FOR CERTAIN SERVICE CONTRACTS SHOULD BE ADDED TO THE FTC'S RULE

Visa strongly urges the FTC to revise its Rule to provide a transition period to allow the continuation of existing contracts with service providers, even if the contracts do not fully satisfy the Rule's requirements. In this regard, the Banking Agency Guidelines provide that until July 1, 2003, a contract that a financial institution has entered into with a service provider satisfies the contractual requirements of the Banking Agency Guidelines even if the contract does not include the contractual provisions set forth in the Banking Agency Guidelines, as long at the institution entered into that contract before March 5, 2001. A similar type of transition period should be added to the FTC's final Rule. It would be virtually impossible for financial institutions to reevaluate and renegotiate instantaneously all of their existing contracts with service providers to incorporate contractual provisions dealing with security. Experience shows that this renegotiation is not a simple process; boilerplate language offered by the financial institution may not be automatically accepted by the service providers.

The FTC should provide financial institutions with a reasonable transition period during which to bring their existing contracts into compliance with the contractual requirements of the FTC's Rule.

* * *

Again, we appreciate the opportunity to comment on this important subject. If we can assist you further, or if you have any questions regarding the above, please feel free to call at 415/932-2178.

Sincerely,

Russell W. Schrader