



October 6, 2000



By Electronic Delivery

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

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

Dear Sir:

This comment letter is submitted on behalf of Visa U.S.A. Inc. ("Visa") in response to the Advanced Notice of Proposed Rulemaking issued by the Federal Trade Commission (the "Commission") 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 Payment System, of which Visa U.S.A. is a part, is the largest consumer payment system in the United States and in the world, with more volume than all other major payment cards combined. Visa is part of a worldwide association of over 21,000 financial institution members that individually offer Visa-brand payment services. In fact, Visa now has over one billion cards circulating worldwide. These Visa-branded cards are held by consumers around the globe, and generate over \$1.6 trillion in annual volume worldwide and over \$700 billion per year in the U.S. At peak volume, Visa's system processes over 3,800 card-related transactions per second. In 1999, the Visa network processed 11 billion credit card transactions worldwide.

GENERAL COMMENTS ON THE PROPOSED RULE

As a general matter, Visa urges the Commission to follow the approach set forth in the federal banking agencies proposed Guidelines, which establish a general framework focusing on the "process" that financial institutions should follow in designing and implementing an information security program, without attempting to specify in detail how a financial institution should structure its information security

program.¹ This “general framework” approach would meet the Commission’s obligations to implement the standards prescribed under Section 501(b) of the GLB Act and would provide 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.

PROPOSED SECURITY STANDARDS SHOULD BE CONSISTENT WITH PROPOSED FEDERAL BANKING AGENCIES’ GUIDELINES

The Commission solicits comment on various issues, such as what constitutes consumer information and what are appropriate security standards. For all matters that will be addressed in its proposed Rule, it is essential for the Commission to strive to ensure uniformity with the proposed federal banking Guidelines. The Commission and the banking agencies provided uniform final privacy rules, and the same approach should be taken in addressing security standards. Consistency among all agencies is critical to minimize compliance burdens for financial institutions.

The proposed Guidelines properly recognized that the types of administrative, technical and physical safeguards that are appropriate for a financial institution to adopt to protect the security of customer information depend on a variety of factors that vary from financial institution to financial institution -- the size and complexity of the institution and the nature and the scope of its activities. The Commission should also recognize this need and allow this flexibility in its proposed Rule.

In addition, the Commission has solicited comment on whether to require minimum security standards and procedures. We do not believe such guidance is necessary or appropriate. Appropriate security standards are likely to change with technology and other developments, and requiring such standards or procedures could be unnecessarily onerous on financial entities. Flexible standards are needed in such a dynamic industry. Furthermore, such guidance would likely be inconsistent with the banking agencies Guidelines, since the Guidelines did not raise such issues. These inconsistencies would be particularly burdensome for entities that have affiliates subject to the Commission’s rules and others subject to the banking agencies’ Guidelines. Thus, we urge the Commission to develop its proposed Rule to ensure uniformity with the banking agencies Guidelines.

DEFINITIONS

Definition of “Customer” and “Customer Records”

The Commission requests comment on how the proposed Rule should define “customer records and information” and whether the Rule should require financial

¹ On June 26, 2000, the Office of the Comptroller of the Currency, Federal Reserve Board, Federal Deposit Insurance Corporation and Office of Thrift Supervision proposed Guidelines to implement Section 501 of the GLB Act.

institutions to safeguard both customer and consumer records. For the reasons discussed below, the Commission should use the definition of "customer" provided in its final privacy rules.

The term "customer" should not include business customers or consumers who have not established an ongoing relationship with the financial institution. The Commission should not expand the scope of the Rule beyond the parties covered by the statute to apply to business customers of financial institutions. Congress -- in passing the privacy provisions in Title V of the GLB Act, including Section 501 -- did not intend to extend the coverage of the Act to business customers of financial institutions. Instead, Congress correctly recognized that businesses are capable of handling their own transactions without additional protection from the government.

In addition, the scope of the proposed Rule should not cover records regarding all consumers who are not also customers. Limiting the scope of the proposed Rule to the records of consumer "customers" is consistent with the plain language of Section 501. Specifically, Section 501 provides that the Agencies should adopt appropriate standards for financial institutions relating to administrative, technical and physical safeguards to ensure the security and confidentiality of "customer" records and information.

As the Commission recognized in its request for comment, Congress distinguished in the privacy provisions of the GLB Act between "customers" (*i.e.*, those individuals who have an ongoing relationship with a financial institution) and other "consumers" (*i.e.*, those individuals who have obtained a financial good or service from a financial institution for personal, family or household purposes, but who have not established an ongoing relationship). By using the term "customer" in Section 501, Congress clearly intended the obligations of Section 501 to apply only to individuals with whom a financial institution has an ongoing relationship. Requiring a financial institution to apply the Rule to the records of all "consumers" -- regardless of whether they have an ongoing relationship -- would expand the requirements of the statute beyond those mandated by the plain language of Section 501.

In addition, because the final privacy rules impose different obligations under Sections 502 and 503 on financial institutions with respect to "customers" and "consumers," some financial institutions may decide it is best to segregate information regarding "customers" from information regarding other "consumers," such as by creating separate databases. Because financial institutions are just now in the early stages of implementing the final privacy rules, institutions may not know at this point whether they will want to ultimately segregate "customer" information from other "consumer" information and whether different security standards are appropriate. As a result, the Commission should specify in the proposed Rule that the security standards only apply to information relating to consumers who are also customers of the institution.

STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

Objectives of an Information Security Program

In the Advance Notice, the Commission describes the objectives for an information security program as ensuring the security and confidentiality of customer information, protecting against any anticipated threats or hazards to the security or integrity of such information and protecting against unauthorized access to or use of customer information that could either: (1) result in substantial harm or inconvenience to any customer; or (2) present a safety and soundness risk to the institutions. The Commission specifically requests comment on whether "unauthorized use" and "unauthorized access" should be defined. We believe it would be very difficult to define these terms in a way that would provide meaningful guidance and would reflect the wide variety of situations that might involve, or might not involve, unauthorized use of information. Rather than defining these terms, the Commission might explain that unauthorized access to or use of customer information does not include access to or use of customer information with the customer's consent. For example, the Commission could make it clear that if a customer provides his access device or code (such as PIN or password) to an entity and that entity accesses the customer's information using this access device or code, this access to the customer's information by such entity is not an unauthorized access of customer information.

DEVELOPMENT AND IMPLEMENTATION OF INFORMATION SECURITY PROGRAM

Involvement of the Board of Directors and Management

The Commission also requests comment on whether and to what extent the proposed Rule should be similar to the Guidelines for the development and implementation of information security programs. Under the Guidelines, a financial institution's Board must: (1) approve the institution's written information security policy and program; and (2) oversee efforts to develop, implement and maintain an effective information security program, including the regular review of management reports. We believe the Commission should adopt a similar approach so that uniform provisions apply to all financial institutions, regardless of which federal agency is responsible for ensuring compliance with the standards.

To the extent the Commission's proposed Rule recognizes that a financial institution's Board should be involved in the development of the institution's information security program, the proposed Rule should provide a financial institution with the flexibility to determine the proper level and frequency of involvement of the Board. In addition, the proposed Rule should provide a financial institution's Board with the flexibility to determine how best to carry out its duty to be involved in the development of the institution's information security program. For example, the Commission should make it clear in the proposed Rule that a financial institution's Board may delegate to a committee of the Board primary responsibility for involvement

in the institution's security programs, rather than have the entire Board actively involved throughout the process.

The Commission also should clarify in the proposed Rule that a financial institution's Board is not required to designate a single Corporate Information Security Officer or other responsible individual who would have the authority and responsibility, subject to the Board's approval, of developing and administering the institution's information security program. Instead, the Commission should make it clear that a financial institution has the flexibility to determine how best to structure its management team for its information security programs. While many financial institutions may have one person -- such as an Information Security Officer -- who is responsible for developing and administering the institution's information security program, other financial institutions may decide it is best to create a working group or committee for this purpose.

Anticipated Threats and Hazards to the Integrity of Customer Records

The Commission requests comment on whether customers should be granted "periodic access" to their records in order to monitor the accuracy of such information. We do not believe that a customer should be granted periodic access. Section 501 does not create any independent substantive right of customers to have "access" to information that relates to them, nor do the final privacy rules impose access requirements. We believe this addition would expand the requirements of the statute beyond those mandated by the plain language of Section 501.

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 650/432-3111.

Sincerely,

A handwritten signature in black ink that reads "Russell W. Schrader". The signature is written in a cursive style with a large, prominent "R" at the beginning.

Russell W. Schrader