Russell W. Schrader
Associate General Counsel
and Chief Privacy Officer

December 22, 2011

By Electronic Delivery

Office of the Secretary, Room H-113 (Annex E)
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Re: COPPA Rule Review, 16 CFR Part 312, Project No. P104503

Ladies and Gentlemen:

This comment letter is submitted on behalf of Visa Inc. ("Visa") in response to the Federal Trade Commission's request for comment on its proposed revisions to the Children's Online Privacy Protection Rule ("Rule"). Visa is a global payments technology company that connects consumers, businesses, financial institutions, and governments in more than 200 countries and territories to fast, secure, and reliable digital currency. Although Visa does not target any of its online properties or services to children, or knowingly collect personal information from them, Visa devotes substantial resources to the privacy and protection of consumers' personal information. Visa has, for example, taken an active role in advancing payment products and technologies aimed at ensuring that the payment system operates securely and cardholder data is protected.

Visa appreciates the Commission's invitation to interested stakeholders to comment on the proposed revisions to the Rule. We welcome the opportunity and look forward to a final rule that provides appropriate protection to children without unnecessarily burdening businesses.

A more tailored approach to the regulation of persistent identifiers for non-support functions would protect children's privacy without chilling routine internal data uses.

The Commission proposes to revise the Rule's definition of "personal information" to include persistent identifiers, when they are used for functions other than support for the internal operations of a website or online service. Before using a persistent identifier for such functions, a covered website or online service would have to obtain verifiable parental consent. The proposed Rule defines "support for the internal operations of a website or online service" as "those activities necessary to maintain the internal functioning of the website or online service,

Visa
P.O. Box 8999
San Francisco, CA 94128
U.S.A.

t. 650-432-1167
f 650-432-2145
rschrade@visa.com

to protect the security or integrity of the website or online service, or to fulfill a [permitted] request of a child." The potential scope of this definition is extremely broad, covering many business practices that, while not strictly "necessary to maintain the internal function of the website or online service" are nonetheless generally expected by consumers and, moreover, privacy neutral. For instance, a website may use persistent identifiers to measure the effectiveness of an advertising campaign or to provide site analytics. A business may also use persistent identifiers for fraud or risk control purposes. In its 2010 preliminary report on protecting consumer privacy, Commission staff acknowledged that choice should not be required for many commonly accepted data uses, and it appears that the Commission sought a similar approach here; however, neither the definition nor the Commission's commentary on the proposed Rule provide businesses with sufficiently precise guidance. As a result, the proposed standard – and resulting ambiguity – would leave businesses with the options of non-compliance (and the risk of an enforcement action), the implementation of costly compliance mechanisms (if technically feasible), or the abandonment of routine internal business functions that provide benefits to the site and its users, are not unexpected by parents, and present little, if any, risk of harm to the privacy of users, including children.

To avoid this ambiguity and the risk of chilling legitimate, privacy-neutral internal business practices, Visa respectfully suggests that the Commission decline to incorporate persistent identifiers into the Rule's definition of "personal information" and instead revise the Rule to directly address the specific conduct that raises privacy concerns. The Commission's commentary on its proposed revision suggests that its goal was to prohibit, without prior parental consent, the compilation of data about children through online tracking, including for behavioral advertising purposes.[1] Assuming that is the case, then the Commission should prescribe rules for particular uses of persistent identifiers that are associated with children. For example, it could require parental consent before information is collected from a child for online behavioral advertising purposes. By focusing on the misuse of personal information, the Commission can achieve its goal of protecting children without creating obligations which may have unforeseen consequences.

[1] The Commission's commentary to the proposed Rule suggests that the uses of persistent identifiers that do not qualify as "support for the internal operations of the website or online services" are those that involve the compilation of data about a child. Specifically, the Commission explains: "The Commission believes that when a persistent identifier is used only to support the internal operations of a website or online service, *rather than to compile data on specific computer users*, the concerns underlying COPPA's purpose are not present." Similarly, the Commission's two examples of practices that would not fall within the "internal support" definition both involve the compilation of data on users: "amassing data on a child's online activities" and "behaviorally targeting advertising to the child." 76 Fed Reg. at 59812 (emphasis added).

The categorization of geolocation as "personal information" would not increase privacy protections and would probably decrease them.

The Commission proposes to include precise geolocation within the Rule's definition of "personal information," even absent any combination with name or contact information. This proposal could have the unintended consequence of providing less, not greater, protection to children's privacy.

Precise geolocation information is already considered "sensitive" by industry, and its collection is therefore generally treated as subject to affirmative consent and appropriate security protections. One way for a business to secure such data is to maintain it separately from any personally identifiable information, such as user name, email address, or phone number. In this way, geolocation cannot be linked to an identifiable user. If, however, the Rule's definition of personal information is revised to include geolocation, a covered business would have to flag it as such so that it could ensure that it is used, disclosed, and maintained in compliance with the Rule. The most reasonable way to accomplish this would be for the business to keep all personal information relating to one child together, in one profile – and, in so doing, personalize sensitive information and increase the risks associated with a breach.

In light of these unintended but increased risks, Visa respectfully urges the Commission to take an approach that would achieve the Commission's objectives without exposing children to such risks. For example, instead of including geolocation within the Rule's definition of "personal information," the Commission could revise the Rule to limit the collection and use of children's geolocation information to specified purposes, require that it be kept anonymous, for example, by converting precise geolocation to a zip code, or require that it be deleted within a prescribed period of time.

* * * *

Visa appreciates the opportunity to comment on this important matter. If you have any questions concerning these comments or if we can otherwise be of assistance, please do not hesitate to contact me at (650) 432-1167.

Sincerely,

Russell W. Schrader
Associate General Counsel and Chief Privacy Officer
Visa Inc.