



Russell W. Schrader
Associate General Counsel
and Chief Privacy Officer

January 28, 2011

By Electronic Delivery

National Telecommunications and Information Administration
U.S. Department of Commerce
Room 4725
1401 Constitution Avenue, N.W.
Washington, D.C. 20230

Re: Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework

Ladies and Gentlemen:

This comment letter is submitted on behalf of Visa Inc. (“Visa”) in response to the Department of Commerce Internet Policy Task Force’s proposed Dynamic Privacy Framework, published in the Federal Register on December 21, 2010. 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. Visa devotes substantial resources toward ensuring that its network operates securely, conveniently, reliably, and efficiently, in order to benefit all parties to a transaction and contribute to economic growth. To that end, Visa has taken an active role in advancing new payment products and technologies and securing the payment system. For example, Visa developed the standard that is now known as PCI-DSS, a detailed information security specification directed at better protecting cardholder information.

Visa applauds the Task Force’s involvement of all interested stakeholders in crafting a privacy framework that provides appropriate protections to consumers while not unnecessarily burdening businesses or stifling innovation. We appreciate the opportunity to comment on this important matter.

Tailored Use Of FIPPs Can Provide Significant Protections

The Task Force’s proposed privacy framework includes policy recommendations grounded in Fair Information Practice Principles (FIPPs). Visa agrees that the Task Force should encourage businesses to incorporate applicable FIPPs into their data processing practices but cautions that it

should not abandon the focused protections provided to consumers regarding more sensitive information. As we described in our June 14, 2010 letter in response to the Task Force's Notice of Inquiry,¹ the universal imposition of FIPPs requirements for all data types would impede the free flow of information in unintended and unexpected ways – the consequences of which would include a limitation on the products and services offered to consumers, stifled innovation, and the creation of obstacles to the ability of U.S. companies to compete globally. Additional considerations include the difficulty and costs of integration with legacy products and systems, differentiating on-line and off-line expectations and permissions, and the potentially confusing role of servicers. All of these are contrary to Commerce's mandate of advancing economic growth and would come, moreover, without substantive protections for consumers' privacy. In our view, the U.S. government should encourage the use of FIPPs and continue to target regulation to those categories of personal data it has identified as particularly sensitive and those data practices demonstrated to cause substantial harm to consumers.

Congress has taken this approach with respect to consumer financial information, which has been deemed particularly sensitive, and, as a result, deserving of greater protection. It has enacted a number of measures that are narrowly tailored to protect specific privacy interests, but that also take into account both the legitimate need of financial institutions for free flow of information and the business realities of how such institutions operate. For example, the Gramm-Leach-Bliley Act includes detailed and comprehensive limitations on financial institutions' ability to share their customer information with nonaffiliated third parties.² In addition, the Fair Credit Reporting Act (FCRA) was enacted in 1970 to address a specific concern: namely, the dissemination of incorrect consumer credit reports.³ It regulates, among other things, the disclosure of credit reports by the consumer reporting agencies that aggregate the information and the use of the information by financial institutions and others. In crafting the financial privacy laws, Congress and the regulators struck a balance.⁴ They determined that every law did not have to provide the same rights and obligations. For instance, some, such as the FCRA, provide access and correction rights to ensure that information is accurate. Others set forth different, context-appropriate means of providing transparency and the opportunity for data correction (*e.g.*, via the issuance of periodic statements).

¹ The letter is available at <http://www.ntia.doc.gov/comments/100402174-0175-01/comment.cfm?e=D532E359-81FF-4757-9BEC-4DB0B4E0660E>.

² 15 U.S.C. § 6801 *et seq.*

³ 15 U.S.C. § 1681(a).

⁴ Federal protections for consumer financial information are also contained within the Electronic Funds Transfer Act, the Equal Credit Opportunity Act, and the Fair Credit Billing Act. Together, these laws subject covered entities to a detailed array of privacy obligations and limitations. They have been designed to complement each other, based on an understanding of the ways in which covered entities operate.

Not All FIPPs Are Appropriately Applied To Entities That Do Not Directly Interact With Consumers

Companies that have direct relationships with consumers should be encouraged to incorporate FIPPs into their products and data processing practices. The Task Force should also recognize, though, that it is not realistic (from either a business or consumer perspective) for companies without direct consumer relationships to adopt all FIPPs for all data types. For example, Visa's network affords consumers the convenience of making digital payments to both online and offline businesses, but Visa itself does not issue payment cards, extend credit, set rates and fees, or otherwise generally interact with consumers as part of payment processing. Rather, the banks who are members of the Visa network issue payment cards, collect fees, set rates, and interact directly with consumers. As a practical matter, then, it would be difficult and inefficient for Visa and others in similar intermediary roles to apply FIPPs to the consumer data they process.

The notice and choice FIPPs, in particular, raise complicated issues. Visa strongly supports the concept of transparency, but Visa is not in the position to provide notice or choice to consumers. Visa, in its role as intermediary, would not ordinarily contact a consumer, and a consumer may have no occasion to interact directly with Visa. Moreover, if Visa were to contact consumers directly, it would likely create confusion and would duplicate the notice and choice already provided by the financial institution that deals directly with the consumer. The issuer – not its intermediary – is in the best position to comply with the notice and choice FIPPs. This issue is exponentially magnified if an issuing financial institution and a merchant use other aggregators and processors at other steps of the way when providing a single service to a cardholder.

Conversely, an intermediary such as Visa is in an excellent position to abide by the security FIPP. In fact, Visa has shown significant leadership in data security throughout the payment chain of merchants and processors. Intermediaries to whom personal information is entrusted should be expected to protect personal information. For these reasons, Visa respectfully requests that the Task Force clarify that intermediaries are not subject to all of the FIPPs provisions of any final privacy framework, but only those that appropriately reflect the role that an intermediary plays in processing personal information.

Privacy Impact Assessments Should Be Encouraged But Not Required

Commerce proposes that companies be required to conduct Privacy Impact Assessments (PIAs) to identify, evaluate, and mitigate risks arising from the use of personal information in new practices or technologies. PIAs are valuable tools. Their use should be encouraged, but it should not be mandated. Full-blown PIAs are not appropriate for every new practice or technology; rather, a detailed PIA is especially appropriate when there is a serious risk of negative and unknown consequences to privacy. When the consequences are already known and certain measures and procedures are commonly applied to address them, then applying a risk-based

model suggests a simpler PIA is sufficient. In addition, the triggers for updates or validations of PIAs should be determined by the company itself so that overly broad PIA mandates do not become another costly and unnecessary administrative burden.

Requiring PIAs to be made public may discourage their use and possibly compromise their integrity. First, bad actors could access and use a company's PIA to exploit the weaknesses in its security operation (as described in the PIA itself). Second, if PIAs are made public, companies may be discouraged from making honest assessments to identify risks and creating risk mitigation techniques. PIAs are useful precisely because they can identify risks during the product development process. To the extent risks are identified, the company can address them before a product is made commercially available. This benefit would be lost if companies were forced to disclose the reports.⁵ Finally, a requirement that PIAs be publicized could expose a company's trade secrets. While the public-facing aspects of a product can often times be readily discerned, the back-end operation of such products, which can typically be the focus of a PIA, are not. The back-end operation can reflect the most innovative and creative aspects of a new product. As a result, a public-disclosure requirement would be likely to create a disincentive to the use of PIAs. Their value as a powerful internal tool enabling a company to manage and mitigate its risks would be severely undermined.

Employee Data Should Not Be Subject To All FIPPs Obligations

We believe that different rules should apply to employee data than apply to consumer data. Organizations collect personal information from their employees to fulfill their employer obligations and carry out legitimate business activities. When information is collected, used, and disclosed for such purposes, the full complement of FIPPs should not be applied. For example, while it is extremely important to protect employees' personal information, choice should not be required to collect, use, and disclose it for legitimate and/or reasonable purposes within the context of the employment relationship and any subsequent retiree relationship (which purposes may vary depending on the business and industry sector of the organization). If, however, an organization wishes to collect, use, and disclose employee data for purposes beyond those that are legitimate and/or reasonable within the context of the employment relationship, then employee choice may be appropriate.

* * * *

⁵ By way of analogy, bank examiners' reports are both detailed (and therefore useful) and protected against disclosure.

January 28, 2011

Page Five

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 in connection with this matter, please do not hesitate to contact me at (650) 432-1167.

Sincerely,

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