Russell W. Schrader
Associate General Counsel
Global Enterprise Risk

June 14, 2010

By Electronic Delivery

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

Re: Information Privacy and Innovation in the Internet Economy

Ladies and Gentlemen:

This comment letter is submitted on behalf of Visa Inc. ("Visa") in response to the Department of Commerce ("Commerce") Internet Policy Task Force's Notice of Inquiry ("Notice") relating to privacy and the Internet economy, published in the Federal Register on May 10, 2010. Visa operates the Visa payment card network, which is the largest consumer payment system and the leading consumer e-commerce payment system in the world. Visa plays a pivotal role in advancing new payment products and technologies, including technology initiatives for protecting personal information and preventing identity theft and other fraud. We appreciate the opportunity to comment on this important matter.

Commerce Should Play a Leading Role in the Global Privacy Debate

Commerce should play a leading role in representing the interests of U.S. businesses in domestic and international discussions to ensure that individual privacy interests are respected within the world's information-driven economy. Over the years, a number of federal agencies have represented the U.S. in global privacy discussions. Commerce, however, has significant policy responsibility for growth and innovation in the U.S. economy. Specifically, Commerce's mandate is to advance economic growth and jobs and opportunities for the American people. As the U.S. and global economies grow far more dependent on information, any new limitations on how businesses may handle information can have a significant impact on economic growth. As a result, Commerce should be a leading voice representing U.S. interests in global privacy discussions.

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

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

Moreover, Commerce should continue to support global policy frameworks that assure that information flows throughout the world without impediments, but with oversight and governance. Current global privacy frameworks that are being discussed, such as the APEC Privacy Framework and the OECD Privacy Guidelines, will evolve over time. It is important that the U.S. government be a part of the process and actively contribute to this evolving area. In addition, these frameworks work best when there are common objectives for data protection. In this regard, Commerce should lead a process involving international industry stakeholders to develop these common objectives.

With respect to the Internet specifically, Commerce should help provide the U.S. government's vision for an innovative but safe Internet that bolsters our information-driven economy. Innovation comes from understanding data, including personal information, and using that understanding to improve business processes. Business processes are diverse, ranging from logistics to risk management and fraud prevention to business continuity. The benefits of improved business processes are unquestioned. Nonetheless, innovative uses of information must be compatible with responsible and answerable personal information management. The U.S. should be a leader in finding innovative ways to protect privacy and enhance data security while encouraging the free flow of information in a globally connected economy.

Commerce Should be Cautious of Overly Broad Regulation

Commerce and the U.S. government should be particularly cognizant of the balance that must be struck between innovation and regulation. In this regard, overly broad regulation tends to stifle innovation, and, with respect to privacy, tends to do so without actually protecting consumer privacy interests in a substantive manner.

Moreover, if U.S. companies are subjected to an overly broad privacy regime, they will likely be put at a competitive disadvantage with respect to their global competitors. For example, inconsistent and often contradictory limitations on cross-border data transfers of personal information can place companies at an immediate disadvantage. These limitations prevent businesses from providing the products and services that their customers demand and from managing their global operations in an efficient and cost effective manner. Global data flows have become a common and essential component of our daily lives and restrictive cross-border data transfer limitations create artificial barriers to trade without enhancing privacy protection for consumers.

The U.S. should avoid the pitfalls that we have seen with other data protection laws that put procedural requirements ahead of strategic management and protection of information. Large multi-national businesses rely on global data flows in order to comply with legal and regulatory obligations such as risk control and fraud prevention. For many global financial businesses, moving and centralizing data around the world is critical to effectively identifying, assessing, monitoring and managing risk. Moreover, global data flows are essential to preventing fraud,

money laundering and terrorist financing. In fact, existing U.S. privacy laws include exceptions to limitations on sharing personal information because they recognize the critical need to ensure data flows for precisely these purposes.

As a leader in information security standards and a provider of important anti-fraud tools, Visa relies on cross-border data flows. For example, Visa deploys cutting-edge technologies to monitor payment card transaction on a global basis—24/7/365—in order to spot fraud the moment it occurs and stop it. Our sophisticated neural networks flag unusual spending patterns that enable financial institutions to block authorizations for payment card transactions where fraud is suspected. These important fraud prevention tools, however, cannot be utilized on a global basis without cross-border data flows. Similarly, other businesses must be able to manage their global operations effectively and transfer both personal information, such as customer and employee data, as well as general business information, such as technical data, to their operations around the world in order to prevent fraud and ensure that consumer information is protected. Rules that limit businesses ability to effectively and efficiently prevent fraud or manage their business will stifle innovation, hurt U.S. business and will not lead to greater protection of consumers.

Other Privacy Considerations

In considering privacy and the Internet, there are a number of important considerations that should be weighed in developing a vision for an innovative but safe Internet and information-driven economy.

- Any new privacy framework or protection should preempt state laws and, in so doing, create a uniform national standard. If any changes are adopted, those changes should provide for a single national standard will provide all American consumers with the same protections no matter where they may reside. In addition, a single national standard will provide covered businesses with just one standard with which they must comply. If a federal a law is adopted that does not preempt state laws, the result will be inconsistent or conflicting standards. Moreover, businesses would have to adopt complex compliance plans based on where they operate or where their customers reside.

- In addition, any new privacy framework or protection should preserve the values that are derived from regulating privacy with an understanding of the industry to which that framework or protection will apply. Where there are strong sectoral regulators, those regulators should be responsible for oversight for the particular industry. For example, financial institutions, including banks, credit unions and broker-dealers, are subject to examination and oversight by various federal financial regulatory agencies.

The privacy issues that the U.S. Government is considering are complex. Moreover, working through these privacy issues across business models, technologies and industries will be both

time consuming and difficult. Nonetheless, the process is worth the effort and difficulty. Ultimately, consumers drive a significant portion of the U.S. economy. Visa works everyday to protect the trust of the consumers who carry Visa-branded payment cards, including through robust privacy and information security programs and practices. Visa would value the opportunity to work with Commerce to foster greater consumer trust in the use of their data, while also fostering innovation in both technology and business models that has made the U.S. economy the envy of the world.

* * * *

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 Schrader
Associate General Counsel and Chief Privacy Officer
Visa Inc.