VISA

Russell W. Schrader
Senior Associate General Counsel
Global Enterprise Risk
Chief Privacy Officer

December 13, 2013

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive
Stop 8930
Gaithersburg, MD 20899
(Delivery via e-mail to cyberframework@nist.gov)

RE: Request for Comments on the Preliminary Cyber Security Framework

Dear Ms. Honeycutt:

Visa appreciates the opportunity to respond to the National Institute of Standards and Technology ("NIST") Request for Comments on the Preliminary Cyber Security Framework (the "Preliminary Framework"). Visa supports the efforts of NIST and the Administration to better secure our nation from cyber attacks through increased public and private sector cooperation. We hope that our perspectives may help guide government and industry efforts to better cooperate on a national cyber security framework.

Visa supports NIST's efforts to engage the industry in developing the Preliminary Framework. Government and industry have a common interest in cyber security. Critically, cyber security requirements vary across business sectors and among individual organizations within each sector. Visa is one of many organizations operating in a complex, diverse financial services sector, and a "one size fits all" approach will not work for all organizations in the financial services sector, let alone across business sectors. At the same time, Visa's efforts to maintain a secure infrastructure in the face of cyber threats can benefit from the experience of other sectors' and other organizations' experiences, as well as the experience of the public sector. NIST can play a critical role in assembling and disseminating key information on cyber security.

Public and Private Sector Cooperation

Visa expects that cyber security will always be a top priority. Our company has helped build the electronic payments ecosystem over more than 50 years, and that ecosystem is founded on a promise to consumers, merchants, and financial institutions that transactions will be securely and efficiently processed. In recognition of the trust placed in us, Visa is diligent in fortifying the security of our systems and the broader payment ecosystem by working with industry organizations, governments, and law enforcement officials.

Visa works closely with government and law enforcement, including with the U.S. Secret Service, Federal Bureau of Investigation, Department of Homeland Security ("DHS"), Department of Defense, National Security Agency, Interpol, and other federal and state agencies, on cyber security issues. Visa provides training, such as the *"Resource Manual for Prosecutors and Investigators,"* to help law enforcement better understand the payment system and financial crimes. Additionally, we maintain a 24-hour hotline for law enforcement agents to call for assistance in their investigations. Visa believes that these types of coordinated efforts have a significant impact on the ability of law enforcement, and ultimately the economy generally, to thwart increasingly sophisticated cyber attacks and hacker intrusions. Visa encourages NIST to continue to build on existing public sector and private sector working relationships.

In the face of increasingly sophisticated cyber attacks, the federal government is uniquely positioned to encourage and improve information sharing regarding threats, vulnerabilities, and controls. Visa supports NIST's efforts to share information with private industry, between government agencies, and across international institutions. Improved information sharing is core to the success of enhancing cyber security across industry sectors, and Visa supports improving and broadening the sharing of confidential information to help thwart cyber attacks. Although critical infrastructure may present the greatest risks, these improvements should not be limited to entities that maintain critical infrastructure, but should also extend more broadly to other private sector entities. Broader information sharing will avoid cliff effects in risk management where there are significant differences in risk controls between critical infrastructure and other systems, which, in effect, would encourage cyber attacks on systems outside of the scope of critical infrastructure.

Improved information sharing will depend on parties' ability to share information with confidence that it will remain confidential with the recipients and that it can be shared without liability. Such protections will allow government and businesses to exchange specific threat information and defense strategies, secure the nation's cyber assets, and mitigate emerging threats in real time, all with appropriate liability, antitrust, and freedom of information protections. Once cyber threat information is readily shared between the public and private sectors, it will be necessary to expand existing threat-informed risk management and mitigation efforts, as well as sector-coordinating councils and government operations centers. Such steps will better position the public and private sectors to collaboratively combat cyber threats and attacks.

The public and private sectors also can coordinate to improve public education and awareness efforts on cyber security. The DHS's work with the National Cyber Security Alliance to promote the educational campaign "Stop. Think. Connect." leveraged the government's credibility and resources to educate consumers. Visa supports this effort, as well as the U.S.

Cyber Challenge, which aims to significantly reduce the shortage in our country's cyber workforce through accessible, compelling programs for students.

Flexible Frameworks, Standards, Guidelines and Best Practices

Visa payments take place in a complex ecosystem that includes financial institutions, other payment networks, processors, vendors, merchants, and consumers. Visa has worked extensively with various stakeholders within the industry to set clear, *centralized* standards that can be implemented in a *decentralized* fashion.[1] These standards and requirements are thorough and cover logistical, physical, technical and operational elements of security. They have been developed over many years and are constantly being reviewed and updated.

Based on its experience in setting standards for Visa payments, Visa believes that NIST's commitment to a voluntary and flexible framework is appropriate and the only viable approach to cyber security. However, as government seeks to enhance cyber security by centralizing *best practices*, it is important to avoid centralizing *implementation* of security measures across a diverse economy. Mandating specific technologies or solutions can have unintended consequences and inhibit innovation. Suitable, effective security controls in one environment may be unworkable, unnecessary, or even counterproductive in other environments. This is particularly important for companies like Visa with operations around the globe: the ability to globally scale an effort like cyber security is important to avoid confusing, duplicative or contradictory standards.

* * * *

While law enforcement is ultimately responsible for investigating, disrupting, apprehending and prosecuting cyber criminals in the U.S. and abroad, Visa recognizes that America's national and economic security is a shared responsibility and must also be a top priority of government and the private sector. Accordingly, Visa supports NIST's objective of fostering public and private sector collaboration in its efforts to adopt a comprehensive national Cyber Security Framework.

On October 2, 2013, a wide-range of representatives from industry, government, academia and law enforcement attended Visa's Fifth Global Security Summit in Washington, D.C. The need

[1] Visa participates in setting a number of very good cyber security standards that exist today, including: (1) Payment Card Industry Data Security Standards (PCI DSS); (2) EMVCo Standards; (3) International Organization for Standardization (ISO) Standards – ISO 27001 and ISO 27002; (4) Accredited Standards Committee X9 – Financial Services Standards; (5) FFIEC/National Institute of Standards and Technology Requirements – NIST SP 800-53; (6) Financial Services Information Sharing and Analysis Center (FS-ISAC) Best Practices; (7) Sarbanes-Oxley and Gramm-Leach-Bliley Requirements; (8) Control Objectives for Information and Related Technologies (COBIT); (9) Federal Information Processing Standards – FIPS 140-2; and (10) Global Platform Specifications.

for public and private sector collaboration was a regular refrain, and summit participants agreed that the best way to develop such collaboration is through horizontal and vertical information sharing. Only through such information sharing can the industry hope to create a partnership that will thwart cyber attacks.

Visa looks forward to working with NIST, the rest of the Administration, and Congress to combat growing cyber threats in a manner that serves the interests of consumers, businesses, and our entire country.

Sincerely,

Russell Schrader