Russell W. Schrader
Associate General Counsel
Global Enterprise Risk

August 1, 2011

By Electronic Delivery

Internet Policy Task Force
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Washington, D.C. 20230

Re: Cybersecurity, Innovation and 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 request for public comment relating to cybersecurity, innovation and the Internet economy, published in the Federal Register on June 15, 2011. 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.

Cybersecurity is Critically Important

The issue of cybersecurity continues to be of critical importance. The security of information handled on the Internet by legitimate businesses and the consumers who obtain their products and services is constantly threatened. As Commerce has noted, cybersecurity threats include not only attacks to exploit the interconnectedness of the Internet, but also targeted attacks the purpose of which is to steal, manipulate, destroy or deny access to sensitive data. For example, criminals frequently seek to obtain personal information about consumers that can be used to conduct identity theft or fraud. Nonetheless, as Commerce has noted, broad swaths of the U.S. economy do not take advantage of available technologies and processes to secure their systems.

Financial institutions in this country have been at the forefront of information security and cybersecurity innovation. Moreover, unlike most businesses, financial institutions are subject to detailed information security requirements under the federal Gramm-Leach-Bliley Act

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

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

("GLBA").[1] The GLBA is the cornerstone of U.S. law that protects consumer financial privacy and information security. For example, the GLBA and its implementing regulations require that financial institutions implement comprehensive, written and risk-based information security programs that are designed to safeguard customer information. Specifically, a financial institution must develop, implement and maintain a written, comprehensive information security program that includes administrative, technical and physical safeguards that are designed to protect the financial institution's customer information.[2] These safeguards extend to all handling of customer information by a financial institution, including customer information that is transmitted, maintained or otherwise handled on the Internet.

Moreover, the GLBA information security requirements include a number of provisions that are designed to address cybersecurity specifically. For example, the GLBA implementing regulations require that banks consider various security measures and adopt such measures where appropriate. These security measures include access controls on customer information systems, encryption of customer information while in transit or in storage on networks, procedures designed to ensure that customer information systems modifications are consistent with the bank's information security program and monitoring systems to detect actual and attempted attacks on customer information systems.[3] Moreover, the GLBA implementing regulations also require that banks implement programs to respond to security incidents involving customer information, including notifying customers of unauthorized access to customer information in electronic form.[4]

Banks are also subject to other information security requirements, including requirements regarding the Internet banking environment. For example, the federal banking agencies have issued detailed requirements that provide a risk management framework for banks offering Internet-based products and services to their customers.[5] In this regard, banks must use effective methods to authenticate the identities of their customers, and such methods must be commensurate with the risks associated with the products and services offered and the protection of sensitive customer information.[6] Moreover, the federal banking agencies recently updated these requirements to require banks to implement a layered approach to security for high-risk, Internet-based systems.[7] For example, a layered approach may include security controls, such as the use of dual customer authorization through different access devices, the use of out-of-band

---

[1] *See, e.g.*, 15 U.S.C. §§ 6801 – 6809.
[2] *See, e.g.*, 12 C.F.R. pt. 30, App. B (OCC).
[3] *Id*.
[4] *See, e.g.*, 12 C.F.R. pt. 30, App. B, Supp. A (OCC).
[5] Authentication in an Internet Banking Environment, Federal Financial Institutions Examination Council (Oct. 12, 2005), *available at* http://www.ffiec.gov/pdf/authentication_guidance.pdf.
[6] *Id*.
[7] Supplement to Authentication in an Internet Banking Environment, Federal Financial Institutions Examination Council (June 28, 2011), *available at* http://www.fdic.gov/news/news/press/2011/pr11111a.pdf.

verification for transactions and IP reputation-based tools to block connections to banking servers from IP addresses known or suspected to be associated with fraudulent activities.[8]

As a result, financial institutions are subject to substantial requirements surrounding the security of their customer information, including specific requirements related to cybersecurity. Most businesses in the U.S. economy, however, are not subject to similar requirements, even at the state level. In considering potential information security requirements for those industries that are not subject to strong sectoral information security standards, Commerce should consider the GLBA requirements as an appropriate model. Moreover, if the federal government adopts new information security requirements that will apply generally throughout the economy, such new requirements should take into account the existing protections required under the GLBA and the specialized nature of the financial industry, so as not to require overlapping or inconsistent requirements for financial institutions.

Visa Information Security Efforts

Visa is a leader in information security standards and a provider of important anti-fraud tools to other businesses. Ensuring Visa payments are convenient, reliable and secure are Visa's highest priorities. Visa believes that it is critical to maintain and strengthen cardholder trust in every Visa transaction. As a result, Visa protects each link within our control and works with others in the payment chain to ensure there is no single point of failure.

Visa has invested heavily in advanced fraud-fighting technologies, and we continue to develop and deploy new and innovative programs that fight fraud and protect cardholders. For example, Visa deploys cutting-edge technologies to monitor payment card transaction on a global basis—24/7/365—in order to spot fraud when 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. Visa's efforts have kept fraud rates at historic lows, enabling cardholders to use Visa with confidence. In fact, with technological innovations and advances in risk management, fraud rates have declined by more than two-thirds over the past two decades. Moreover, Visa has invested heavily in order to develop and maintain highly secure data centers to protect transaction data.

In addition, Visa is a founding member of the PCI Security Standards Council, which develops the information security standards for the handling of payment card data—the Payment Card Industry Data Security Standard ("PCI DSS"). PCI DSS was developed to encourage and enhance cardholder data security and the broad adoption of consistent data security measures for cardholder data globally. PCI DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers and service providers, as well as other entities that store, process or transmit cardholder data. In this regard, PCI DSS provides a baseline of

[8] *Id*.

technical and operational information security requirements for cardholder data. Many of these requirements are specifically designed to address cybersecurity risks, including, for example, requirements that covered entities install and maintain firewalls to protect cardholder data, encryption requirements for the transmission of cardholder data across open, public networks, anti-virus software requirements, access control requirements and requirements that access to cardholder data be tracked and monitored.

As noted above, Visa's security strategy relies on multiple layers of protection. From anti-counterfeit measures to neural networks that analyze each transaction in real time, Visa takes a total-systems approach to fraud prevention. Visa's fraud prevention efforts focus on: (1) securing the payment environment to protect card data and render it useless in the hands of criminals; (2) managing fraud by protecting cardholders with Zero Liability; (3) maintaining trust through merchant and cardholder education and industry leadership; and (4) creating an environment of partnership by promoting industry engagement and accountability.

Other Considerations

In considering information security and the Internet, Commerce must weigh a number of important considerations to develop its vision for an innovative but safe Internet and information-driven economy. First, any new security framework or protection should preserve the values that are derived from 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.

In addition, any new security 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 that 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 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.

The information security issues that Commerce is considering are complex. Moreover, working through these issues across business models, technologies and industries will be both time consuming and difficult. Visa works everyday to protect the trust of the consumers who carry Visa-branded payment cards, including through robust information security programs and practices. Visa would value the opportunity to work with Commerce to foster greater consumer trust in the security 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

dc-651279