June 2, 2016

By Electronic Delivery

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W., Room 4725
Attn: IOT RFC 2016
Washington, DC 20230

Re: Request for Public Comment; The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things

Docket No. 160331306-6306-01

Ladies and Gentlemen:

This letter is submitted by Visa Inc. ("Visa") in response to the notice published by the National Telecommunications and Information Administration ("NTIA") within the U.S. Department of Commerce ("Commerce"), which requests information about the Internet of Things (IoT) to review the current technological and policy landscape.[1] The Notice and Request for Public Comment ("Notice") is being issued as part of Commerce's Digital Economy Agenda which has set as a top priority the encouragement of growth of the digital economy and ensuring that the Internet remains an open platform for innovation. Comments received in response to NTIA's Notice will inform a subsequent "green paper" by Commerce that would identify key issues impacting deployment of IoT technologies, highlight potential benefits and challenges, and identify possible roles for the federal government in fostering the advancement of IoT technologies in partnership with the private sector.

Visa plays a leading role in advancing payment products and technologies worldwide to benefit hundreds of millions of consumers. Visa does not itself issue payment cards to consumers, but rather it operates the network supporting Visa-branded credit, debit and prepaid card products designed by issuing banks to enable their customers to make purchases at merchants and retailers globally and receive funds in a convenient, secure, and reliable manner. As the web, mobile and social networks converge, and commerce and payments are increasingly becoming digitized, Visa is investing in mobile platforms, technologies, and capabilities to enable consumers around the world to continue to pay, get paid and better manage their finances in the digital

[1] *See* 81 Fed. Reg. 19956 (April 6, 2016).

environment, with the same convenience, security, reliability and global acceptance that Visa has achieved in the physical world. At the same time, we are also extending our network to allow a growing ecosystem of financial institutions, device manufacturers, technology companies, application developers, and mobile network operators to create new, secure and innovative commerce experiences.

How Visa fits into the Internet of Things movement

Connected devices are changing everything we know about shopping and paying – with the web and mobile payments as just the beginning. This next phase of payments is being driven in large part by mobile technology, and new flexible and open payment technologies that enable the creation of innovative, new ways to pay. Consumer behavior is also driving this phase, as consumers embrace mobile technology in order to pay, be paid, and manage their finances.

According to Cisco, the number of IoT enabled devices is expected to reach 50 billion by 2020,[2] providing a huge opportunity for secure payments to be a feature in just about any form factor and anywhere there is an Internet connection. In many regards, connected commerce is already happening today, with the launches of mobile wallets, such as Samsung Pay, Android Pay and others, facilitating the growth of mobile proximity payments using Near Field Communication (NFC) technology and tokenization and the introduction of online ecommerce solutions such as Visa Checkout, that enable consumers to make purchases quickly and easily from their smartphone, tablet, laptop, and PC. Visa has been preparing for this future by developing and providing stakeholders across the payments ecosystem the tools and services they need to foster innovation and allow great ideas to become new ways to pay in a safe and secure manner.

At the heart of enabling payment functionality for IoT devices is tokenization, which Visa has introduced through the Visa Token Service, an innovative security technology that allows for the proliferation of secure mobile and digital payments anywhere there is an Internet connection. Tokenization replaces the traditional payment card account number with a unique digital token, which can be domain restricted for transactions with a specific device, merchant, or transaction type, for example to ensure that a tokenized account credential embedded in a smart appliance is tied to that particular device and cannot be used to authorize ecommerce transactions. In addition, in the event an IoT device with an embedded token is lost, stolen, or compromised, Visa Token Service enables the cardholder's underlying payment card account number to remain secure, thereby eliminating the need to reissue the card. Through Visa Token

[2] Dave Evans, Cisco, *The Internet of Things: How the Next Evolution of the Internet is Changing Everything* 3 (April 2011), *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf .

Service's lifecycle management services, tokens can also be updated if the cardholder's underlying account is lost, expired or compromised.

Access to Visa Token Service and other Visa payment capabilities has been significantly expanded through the launch of the Visa Developer platform which provides developers open access to Visa technology, products and services. With the Visa Developer platform, VisaNet, our global payments network, is being transformed into an accessible platform for payments and commerce to provide developers at merchants, financial institutions, technology companies and startups self-serve access to Visa technologies, products and services for development and testing purposes through simple application program interfaces (APIs) and software development kits (SDKs). Examples of the payment products and capabilities currently available through the platform for test and development include tokenization account holder identification and verification; account validation; person to person payments; real-time and location-based services (e.g., alerts, merchant geolocation and transaction controls); and secure and convenient payment services for online and in-store purchases through Visa Checkout. Providing direct and easy access to Visa technology, products and services through the Visa Developer platform also allows developers to test and integrate multiple Visa APIs into their applications and ensure that their solutions are interoperable with other industry standards APIs and technology platforms commonly used by developers today.

To accelerate the creation of new digital commerce experiences in connected environments, Visa also recently announced the Visa Ready Program for IoT which is intended to enable device manufacturers who want to add payment capabilities to their IoT products and services to launch their solution in market more quickly. Eligible devices in the program could include wearables, automobiles, appliances, public transportation services, clothing and almost any other connected devices. Devices under the Visa Ready Program for IoT will be subject to Visa Ready certification, which helps to ensure that all approved devices meet Visa and EMVCo security and performance guidelines. The Visa Ready certification will provide innovators a path to ensure that their devices, software and solutions can initiate and accept Visa payments with ease and speed. The Visa Ready Program for IoT also provides participants streamlined access to the Visa Token Service and allows a new category of entities to become approved Visa token requestors and request tokens on behalf of their device manufacturer partners.

Benefits and opportunities from the Internet of Things

According to some accounts, IoT could have a potential economic impact of $3.9 trillion to $11 trillion a year by 2025.[3] However, for companies to realize this economic opportunity, policy makers must make sure that they adopt policies and standards that

[3] McKinsey, *The Internet of Things: Mapping the Value Beyond the Hype* 36 (June 2015), *available at* http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

promote innovation, are built around transparency and consumer control, and that do not unduly restrict the ability of companies to deliver solutions that can meet consumer needs and expectations. Visa therefore welcomes Commerce's thoughtful approach to first lead a multistakeholder inquiry into the IoT to seek input on the key issues that policy makers should consider and the appropriate role for the government to foster the advancement of IoT technologies in partnership with the private sector, before issuing specific policy recommendations.

For the payments industry, the potential benefits and opportunities of IoT are several. As payments shift from plastic to digital, the way consumers shop and pay is being transformed from online to mobile to connected device enabling consumers to pay anywhere, on any device, and with any payment account they choose in a secure commerce environment. We envision a future where consumers can seamlessly make many of their everyday purchases not just in store, online at home or at work, or on their mobile devices, but anywhere there is an Internet connection, including their car. Over the past year, Visa has continued to test and evolve the possibilities of in-car payments, including showing how to simplify the process of leasing or buying a car, or even managing services like auto insurance or road tolls, directly from the driver's seat. These "test-and-learn" projects are intended to deliver learnings that will be required to build commercial solutions. Thus, as Visa continues to collaborate and co-innovate, payments stakeholders can utilize these learnings as well as their own to bring secure and convenient payments to a broader number of devices and services. For their part, merchants can similarly take advantage of IoT technologies not just to drive additional sales but also potentially to deliver new offers and rewards to their customers in more environments.

For consumers, in addition to enabling the convenience of being able to pay anywhere and on any device in a secure environment, tokenization technologies can allow their continued access to secure payment instruments with lifecycle management services that can update the tokenized payment credential in case the cardholder's underlying account number is lost, expired, or compromised. Payment credentials are also more secure as domain restrictions on the tokenized payment credential can prevent compromised payment information from being used in a new payment environment. And, IoT technologies can provide a powerful tool for financial inclusion that could provide the underserved an on-ramp into the financial system based around a prepaid platform and access to low-cost electronic forms of financial instruments through everyday devices.

Potential challenges presented by the Internet of Things

As the Internet of Things expands, there is the potential for new payment security vulnerabilities from more connected devices. Just as in the physical point-of-sale (POS) environment, securing electronic payments and fighting fraud must remain a top priority

when developing IoT payments solutions to ensure that consumers can pay with confidence in a safe and secure manner while reducing the threat of sensitive personal account data being compromised regardless of the payment channel or device used.

A key principle to securing the payment system and protecting sensitive data is to limit the amount of data that must be protected, including by removing vulnerable payment data from the merchant environment altogether. To this end, digital wallets can provide consumers a simpler and safer way to pay online from their smartphone, tablet, laptop, or PC without exposing their underlying payment card account information to ecommerce merchants. In addition, tokenization technology enables traditional payment card account numbers to be replaced with a payment "token" in ecommerce and mobile commerce. In addition to removing sensitive account credentials from the payment environment, as noted above, tokens can also be restricted for use with a specific merchant, mobile device, transaction or category of transactions to further enhance cardholder security and confidence in mobile transactions. Although Visa Checkout and Visa Token Service are two important elements to securing commerce in the Internet of Things, these solutions are in addition to VisaNet's robust proprietary risk models which analyze millions of Visa transactions per second to mitigate fraud risks, as part of Visa's multi-layered approach to payment security.

The Federal Trade Commission (FTC) has further observed that the integration of connected devices into everyday life may introduce new privacy risks from the increased collection of personal information, habits, locations, and physical conditions over time, particularly if companies use this data inappropriately.[4] Such risks may have the potential of undermining consumer confidence in IoT and prevent more widespread adoption if not properly managed. In this regard, while some amount of transparency and controls for consumers using connected devices is likely appropriate, perhaps in accordance with the FTC's Fair Information Practice Principles, we would note that overly strict limits on the use of "big data" may lead to unintended consequences and impacts, including the reduction of robust fraud detection capabilities that may rely on the availability of such data.

To ensure IoT technologies are scalable globally and across devices, any technical standards for IoT must allow for flexible and interoperable solutions that can accommodate changing business requirements and consumer needs. To that end, voluntary, global, industry-led open standards (vs. domestic-only specifications) have historically worked well to drive innovation and broad adoption. As an example, EMVCo was created to develop and manage chip card specifications at a global level after domestic-driven chip specifications in the late 1990s had led to domestic designs that were not interoperable across geographic borders, posing challenges to both

[4] Federal Trade Commission, *Internet of Things: Privacy & Security in a Connected World* 14-18 (January 2015), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

businesses and consumers. EMVCo's formation of a global technical body has enabled the development and management of the EMV Specifications which facilitate global interoperability to help all industry participants worldwide to develop and use secure and globally interoperable payment methods. The EMV Specifications are available on a royalty-free basis to all industry participants and to the public, but provide sufficient flexibility to allow individual payment networks to publish their own EMV compliance requirements for implementation. As the payments industry has moved from securing the point-of-sale environment to addressing fraud in other environments, EMVCo has also proven to provide a valuable inter-industry forum for developing specifications for next generation technologies, including the tokenization services that are necessary to facilitate the rapid adoption of IoT devices. For example, the Visa Token Service follows EMVCo's tokenization specification, making it both standard and interoperable across the industry to help enable a new generation of payment products, while maintaining compatibility with the existing payments infrastructure.

Another potential challenge for IoT technologies is the current legal and regulatory structure as the legal framework that governs electronic payments today may not be well suited for IoT devices such as wearables, appliances and other connected devices. Overly rigid application of rules that were developed for a different commerce experience and environment may stifle innovation and discourage investment in IoT technologies. For example, the federal rules for credit and debit cards generally contemplate physical plastic cards, and impose certain disclosure requirements (e.g. disclosures in "writing" or on the "device") that cannot be easily satisfied in a mobile or IoT environment. Commerce should work with the prudential regulators to ensure that a "one size fits all" regulatory approach is not inappropriately applied to emerging technologies and methods of delivery and allow payments regulation to evolve and keep pace with the technologies used to provide consumers the products and services they demand.

Role of government

Visa believes there are a number of roles that the federal government could play in addressing the challenges and opportunities of IoT and collaborate with the private sector to foster the advancement of IoT technologies. First, Commerce should continue to serve as a facilitator of discussions about the policy issues and considerations that arise with the growth and potential impact of IoT, much as it has with the release of this request for public comment and development of the "green paper". In that regard, the Department's prior collective experiences in coordinating the development of a draft reference architecture for Cyber-Physical Systems through its National Institute of Standards and Technology (NIST), and convening of a privacy multistakeholder process through the NTIA to provide a forum for developing a code of conduct around how consumer privacy rights should apply in specific business contexts (e.g. mobile applications), among other initiatives, should serve Commerce well in developing

potential policy recommendations that promote investment and remove barriers to innovation for IoT.

Second, Commerce should coordinate and consult with other regulators, including the FTC, and with legislators, to ensure that multiple governmental stakeholder oversight of IoT does not inappropriately increase regulatory burdens or balkanize regulatory requirements. As noted above, Commerce could also coordinate efforts with other regulators to ensure that regulations do not unnecessarily impede technological developments in the IoT space.

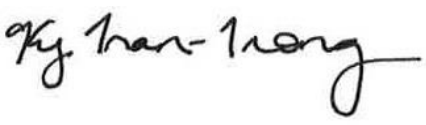
Third, where there are international efforts or forums addressing IoT, Commerce and NTIA should encourage the development of voluntary, global, open industry standards to promote technological best practices and standards that can drive secure, flexible and interoperable solutions that can be scaled globally, avoiding technology mandates. We further note that restrictions on IoT can also be indirectly imposed through privacy regulation or domestic processing regimes. In this regard, we strongly urge NTIA and Commerce to work with the international community to encourage the continued cross-border flow of data to enable IoT services, and discourage any forms of localization or that favor domestic solutions.

* * * *

Visa appreciates NTIA and Commerce's efforts to better understand the current technologies and policy landscape for the IoT. To the extent Commerce believes it would be helpful, Visa would be pleased to meet to share or otherwise discuss its perspective on this critical issue.

If you have any questions, please do not hesitate to contact me at (202) 419-4109 or ktrantro@visa.com.

Sincerely,



Ky Tran-Trong
Associate General Counsel, Regulatory
Visa Inc.