

Smart Card Alliance

Congressional Testimony of Randy Vanderhoof Executive Director, Smart Card Alliance

Before The House Committee on Financial Services,
Subcommittee on Financial Institutions and Consumer Credit on
**The Future of Money: How Mobile Payments Could Change
Financial Services**

***“NFC Contactless Mobile Payments: Technology Proven
Secure and Backed by Wireless and Payments Industry
Leaders”***

March 22, 2012

Chairwoman Capito and Members of the Subcommittee:

On behalf of the Smart Card Alliance and its members, I thank you for the opportunity to testify today. The Smart Card Alliance is a non-profit organization that provides education and a collaborative, open forum among leaders in various industries including mobile payments. The Alliance represents many major stakeholders in the mobile payments ecosystem including payment brands, card issuers, mobile operators, merchants, and technology providers.

We applaud the Subcommittee’s leadership and foresight in examining important issues essential to making mobile payments safe, flexible and resilient with the appropriate legal, regulatory and security frameworks.

The number of American wireless subscriber connections now exceeds the population of the United States and its territories according to industry sources. The total population is 315.5 million inhabitants, while the number of wireless subscriber connections is 327.6 million. Of these, 96 million, almost one out of three, are smartphones and wireless-enabled PDAs that are capable of accessing the Internet and doing much of what people do on their PCs.¹

¹ CTIA - The Wireless Association, "CTIA-The Wireless Association Semi-Annual Survey Reveals Historical Wireless Trend," October 11, 2011 (<http://www.ctia.org/media/press/body.cfm/prid/2133>)



Smart Card Alliance

Over the course of the last ten years, the mobile phone has become the thing people don't leave home without. So it's not surprising that everyone—especially consumers—want to use it for payment and mobile commerce too. Industry forecasts suggest m-commerce is expected to grow 73% in 2012 to \$11.6 billion.²

The 2011 report published by the Federal Reserve Banks of Boston and Atlanta through their Retail Payments Risk Forum points out correctly that there are many ways mobile devices can be used to facilitate the payment process.³ I am going to focus my remarks on just one area that is getting a lot of attention, which is the use of a payment application-enabled mobile phone with a mobile virtual wallet inside that can be used to pay at a physical merchant location as a substitute for a credit or debit card.

This hearing was convened to examine issues essential to making mobile payments safe and to ensure appropriate legislative oversight is in place.

The good news is that for the type of mobile payments that I am talking about, which is using your mobile phone like a payment card, there is a clear mobile technology path forward that achieves these goals because this form of mobile payment is built on already established legal, regulatory and security frameworks in both the payment and wireless telecom industries. In the industry, this mobile technology is referred to as NFC mobile contactless payment. NFC, or Near Field Communication, is a form of short range wireless communications inside a phone.

NFC is a new technology that leverages many layers of existing smart card technology in payment cards (EMV and contactless cards) and wireless mobile devices (SIM cards) and that, together with the existing payment and wireless network infrastructure, enable secure mobile payment at physical merchant locations equipped with NFC-compatible POS terminals.

The NFC mobile contactless payment approach has two advantages very important to this Subcommittee. First, underpinning the legal and regulatory framework is the simple fact that while NFC mobile payments use a phone instead of a card, the payment account remains a credit or debit card account and, as such, is already well-protected for consumers and industry stakeholders by existing laws and regulations. Second, the security and reliability of this approach are grounded in global standards, established certification processes and industry best practices that are the culmination of nearly 20 years of work in applying smart card technology to protect payment accounts and mobile phone subscribers.

² eMarketer, "Smartphones Turn Millions More Americans into Mobile Shoppers," January 6, 2012 (<http://www.emarketer.com/Article.aspx?R=1008769>)

³ "Mobile Payments in the United States: Mapping Out the Road Ahead," Darin Contini and Marianne Crowe, Federal Reserve Bank of Boston, Cynthia Merritt and Richard Oliver, Federal Reserve Bank of Atlanta, and Steve Mott, BetterBuyDesign, March 25, 2011



Smart Card Alliance

I would like to stress that the major stakeholders and technology providers in the financial and mobile industries have been collaborating for years across multiple global standards organizations to add NFC mobile contactless payments to their existing payment and wireless infrastructures. These include:

- NFC Forum, a global standards organization whose members include the leading global payment brands and wireless technology providers
- EMVCo and GlobalPlatform, the former managing the global payments standards for the use of smart card chips in bank cards and now also in phones; and the latter setting standards that facilitate secure and interoperable applications using smart card chip technology in cards and phones, with members including the leading global payment brands and payment technology providers
- The GSM Association (GSMA), consisting of 800 mobile operators and related companies and devoted to supporting and standardizing wireless mobile telephone systems worldwide
- ETSI, the telecommunications standards organization

These organizations have developed the standards for NFC, which are supported by the mobile industry and endorsed by the payments industry, who then applied their own standards, best practices, certification procedures and compliance testing to ensure secure and interoperable NFC mobile contactless payments. The resulting NFC mobile payments ecosystem is safe, flexible and resilient.

The fact that leading payment brands are involved will not only ensure security, it will create trust by consumers and accelerate rapid adoption. According to a recent independent branding study, the brands most trusted by consumers for protecting mobile payments are Visa, MasterCard and American Express.⁴

I'd like to go a little deeper into what NFC is, how it fits into the payments and telecom ecosystems, and why it is secure. NFC technology is implemented in a chipset embedded in mobile phones that enables consumers to transact at a physical point of sale. The technology leverages added security features in the mobile phone and includes something called a "secure element,"⁵ a smart chip protecting the sensitive payment data stored inside the phone as well as managing the execution of the payment transaction by the consumer. In addition, new and existing safeguards in the wireless and payment networks are used with mobile payment devices to add many layers of protection for consumer account information and transactions. For example,

⁴ Kunur Patel, "Survey: Consumers Don't Trust Google or Apple With Mobile Payments," AdAge, August 9, 2011 (<http://adage.com/article/digital/consumers-trust-google-apple-mobile-payments/229163/>)

⁵ The component in a mobile phone that provides security and confidentiality. A secure element can reside on the SIM, in a dedicated chip on a phone's motherboard (embedded secure element), or as an external accessory. The secure element is a smart card chip that contains a dedicated microprocessor with an operating system, memory, an application environment, and security protocols. It is used to store and execute sensitive applications on a mobile device. Source: Smart Card Alliance, "Security of Proximity Mobile Payments," May 2009



Smart Card Alliance

access to the payment application can be password protected and a lost or stolen phone can be turned off instantly with one call to the mobile operator who services that customer.

The Smart Card Alliance has created an educational white paper, "Security of Proximity Mobile Payments," that discusses this subject in detail.⁶

An NFC-enabled phone is provisioned with a version of a payment application (e.g., American Express ExpressPay, Discover Zip, MasterCard PayPass, Visa payWave) and personalized with a payment account (i.e., credit, debit or prepaid) issued by the consumer's financial institution.

To pay, the consumer simply holds or taps the phone close to the merchant's reader. The consumer's account information is sent to the contactless POS reader via radio frequency. The payment and settlement processes are the same processes used when a consumer pays with a traditional contactless or magnetic stripe credit or debit card.

Market development involving many of America's largest and most trusted companies is well underway. One example using the NFC mobile contactless payment technology standards we are discussing here is Isis. This mobile carrier joint venture includes AT&T, Verizon Wireless, and T-Mobile and will work with American Express, Discover, MasterCard, and Visa for its NFC rollouts.

Another example is Google Wallet. Google has already launched its NFC mobile contactless payments offering to consumers, partnering in its initial launch with MasterCard, Citi, First Data, and Sprint. More than two dozen large retailers, including Macy's and American Eagle Outfitters have enabled their stores to accept Google Wallet.

Mobile payments are likely to grow quickly, aided by the rapid rate at which consumers replace their mobile phones with newer technology. Industry watcher Juniper Research predicts NFC payments will hit \$74 billion by 2015.⁷ Sales of NFC handsets in 2012 will reach nearly 80 million units, an increase of 129% from 2011, according to IMS Research.⁸

In summary "the future of money," as this hearing is entitled, is being positively impacted by mobile technology. The changes in financial services that you have

⁶ Smart Card Alliance, "Security of Proximity Mobile Payments," May 2009

(<http://www.smartcardalliance.org/pages/publications-security-of-proximity-mobile-payments>)

⁷ Juniper Research, "Mobile Commerce Market Set to Accelerate with NFC Facilitating \$74bn Transactions by 2015," March 8, 2012 (<http://juniperresearch.com/viewpressrelease.php?pr=291>)

⁸ IMS Research, "35 Million Handsets in 2011 Marks Breakthrough Year for Mobile Near-Field Communications," December 14, 2011 (http://imsresearch.com/press-release/35_Million_Handsets_in_2011_Marks_Breakthrough_Year_for_Mobile_NearField_Communications)



Smart Card Alliance

rightfully called attention to with this hearing are being well-managed and securely protected by the technology and the collective knowledge and resources of the financial and mobile industries.

NFC, the core technology behind mobile contactless payments, was chosen by the mobile carriers and financial industry as the delivery mechanism due to its security and ease of use. The consumer payments applications have been jointly developed on the mobile side by the four largest mobile network brands and on the payments side by the four payments brands, which, according to consumers who were surveyed, were the most trusted for mobile payments in the United States. The path forward has been paved by years of experience.

NFC payment embedded in mobile phones won't be the only form of mobile payment, but this way forward is based on known elements and backed by the mobile operators and payment brands. There are new mobile technologies being tested other than NFC that are promising, yet unproven.

NFC offers many benefits to consumers, both to make payments more convenient and to support new, innovative capabilities that deliver value to both consumers and merchants. Confidence in the underlying infrastructure and credibility of the industry offerings are critical to consumer adoption. Consumers will benefit from a mobile payments infrastructure that is based on a proven set of standards and architectures, has a strong focus on security, and uses the existing payments infrastructure for transactions.

Mobile phones offer a powerful computing platform for innovation and represent a fertile landscape for new ways for consumers to transact with retailers, financial institutions, application stores and each other. Mobile payments innovation is going to continue to evolve and as more people upgrade to smartphones and learn about all of the new services they hold in the palm of their hand. An added benefit of the migration to NFC will be the fact that mobile devices will generally become more secure, because the security technology needed for payment can be used safely for other applications as well.

Conclusion

To sum up, NFC contactless mobile payments as planned by the financial services and wireless industries are basically credit and debit accounts that fit within the legal, regulatory and security frameworks that are serving the public interest today.

The Smart Card Alliance would like to thank the Subcommittee once again for holding this important and forward-looking hearing. Government and industry must maintain an open dialog about legal, regulatory and security frameworks and we greatly appreciate the opportunity to present information that assists in developing options for making mobile payments a reality; in addressing the challenges and opportunities of using



191 Clarksville Road
Princeton Junction, New Jersey 08550 (USA)
1.800.556.6828
www.smartcardalliance.org

Smart Card Alliance

mobile payment systems to exchange value; and in setting the legal, regulatory and security frameworks necessary to implement a safe, flexible and resilient mobile financial product.

We have provided appendices at the end of this written statement to further assist you in examining the mobile landscape as it stands today.

Contact Information

For more information, please contact Randy Vanderhoof, 1-609-587-4208, rvanderhoof@smartcardalliance.org

Appendix A

Mobile NFC Contactless Payment

Appendix B

Glossary



191 Clarksville Road
Princeton Junction, New Jersey 08550 (USA)
1.800.556.6828
www.smartcardalliance.org

Smart Card Alliance

Appendix A – NFC Mobile Contactless Payment

NFC Basics

NFC stands for Near Field Communication and is a standards-based wireless communication technology that allows data to be exchanged between devices that are a few centimeters apart. The technology can be used for a wide variety of mobile applications, including:

- Making payments with a wave or a touch of a device anywhere contactless point-of-sale readers have been deployed
- Reading information and picking up special offers, coupons, and discounts from posters or billboards on which an RF tag has been embedded (for example, in smart posters and billboards)
- Securely storing tickets for transportation, parking access, or events and enabling fast transactions at the point of entry/exit
- Securely storing information that allows secure building access

An NFC-enabled device⁹ can operate in different modes to implement a wide variety mobile applications, including mobile contactless payment.

NFC Mobile Contactless Payment

Contactless payment -- payment with the use of contactless debt and credit cards -- has been a growing market over the past several years. American Express, Discover, MasterCard and Visa branded cards are being issued that contain smart chips that enable contactless payment. The contactless merchant point-of-sale infrastructure that is now in place to support credit and debit payment can also accept NFC mobile contactless payments, providing a head-start for broad acceptance and use.

With NFC, contactless payment capabilities are in the mobile phone, allowing secure storage and use of payment accounts with the mobile phone.

To support mobile contactless payments, the NFC-enabled phone has a smart chip (called the “secure element”) which is loaded with a version of a payment application (e.g., American Express ExpressPay, Discover Zip, MasterCard PayPass, Visa payWave) and personalized with a payment account (i.e., credit, debit or prepaid) issued by the consumer’s financial institution. The phone can then use NFC technology to communicate with a merchant’s contactless payment-capable POS system. To pay, the consumer simply holds or taps the phone close to the merchant’s reader. The consumer’s account information is sent to the contactless POS reader via radio frequency. The payment and settlement processes are the same processes used when a consumer pays with a traditional contactless or magnetic stripe credit or debit card.

⁹ NFC-enabled devices are governed by standards in ISO/IEC (ISO/IEC 18092), ETSI (ETSI TS 102 10 V1.1.1 (2003-03)) and ECMA International (ECMA-340), and by specifications published by the NFC Forum.

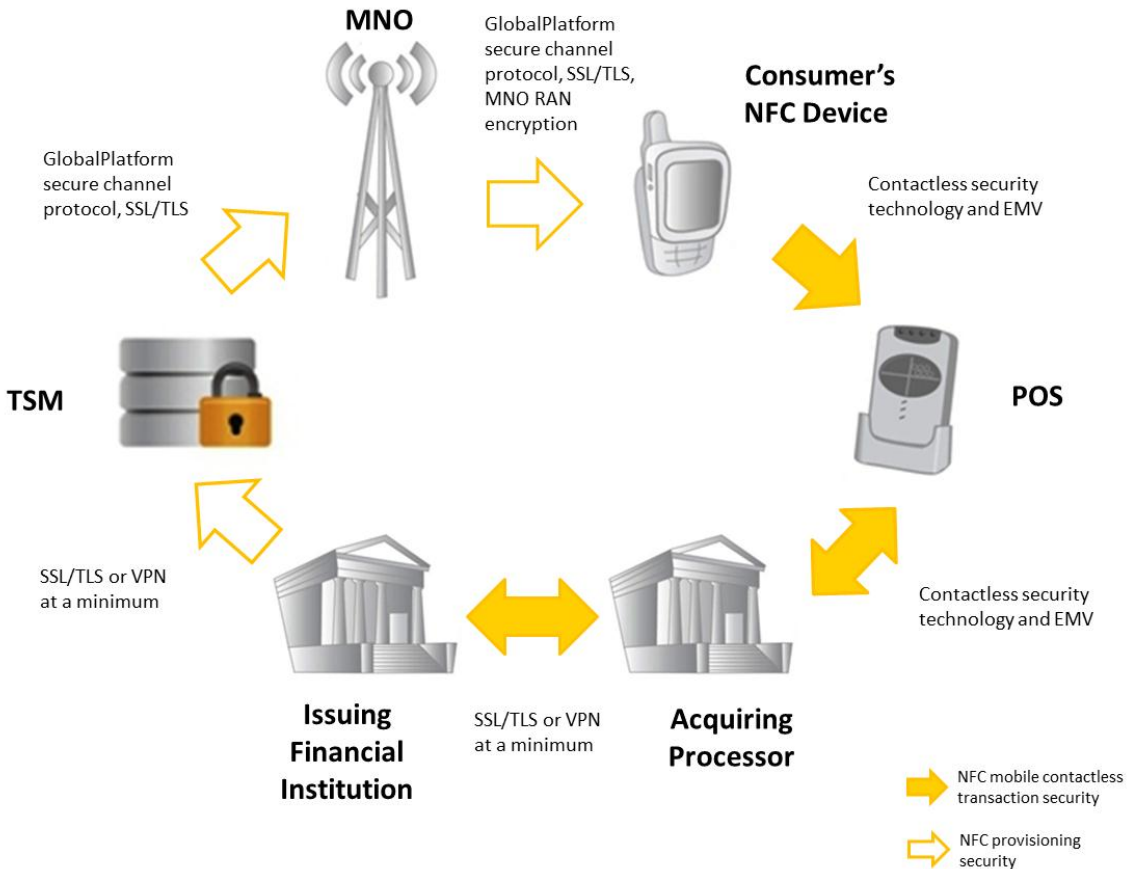


Smart Card Alliance

Currently many NFC mobile payment pilots and initiatives are happening worldwide involving many of the world's largest companies. Most notably in the U.S., Google Wallet is currently available to owners of the Nexus S 4G on Sprint Mobile, and Isis, the joint venture among AT&T Mobility, Verizon Wireless, and T-Mobile USA, has signed up American Express, Discover, MasterCard, and Visa for NFC mobile payments.

The figure below illustrates the security mechanisms that protect the processes used in NFC mobile contactless payments; these mechanisms are described below.

Figure 1. NFC Mobile Contactless Payments Security Mechanisms



Delivering Financial Data Securely

The issuer transmits payment, personalization, and life cycle management information to a Trusted Service Manager (TSM) using standard Internet technologies, such as secure sockets layer (SSL) or virtual private networks (VPNs). GlobalPlatform's secure channel protocol provides for transmission of sensitive account data between the TSM and the secure element in the mobile device and for storage of the information in the phone's secure element. Account data is further kept secure by encryption provided by the mobile network operator (MNO).

Smart Card Alliance

Protecting Stored Payment Application and Account Information

Within the mobile phone, both the payment application and consumer account information must be protected, and different NFC applications must be able to work securely and independently of each other. Security approaches used include:

- Storing the payment application and data in the secure element.
- Using smart card technology that is inherent in the secure element to authenticate all communications with applications and to provide built-in tamper resistance.
- Providing a mobile wallet for accessing the payment account information in the secure element during a transaction, with an optional personal identification number (PIN) authorizing access to the wallet.

Protecting the Payment Transaction

When the consumer uses the NFC device for payment, the transaction is protected using the same security mechanisms in place for contactless credit and debit cards. Payments are processed over the current financial networks and use the payments industry security infrastructure. Security approaches used include:

- Leveraging existing issuer host system payment transaction authorization technology and account management processes.
- Protecting the transaction using the dynamic cryptogram authentication technology that is already in place for contactless credit and debit cards.
- Leveraging EMV contactless card transaction authentication security technology.

NFC and EMV

The global payments industry is migrating to the next generation payments infrastructure based on smart chip technology and the EMV specifications¹⁰. EMV is an open-standard set of specifications for payments and acceptance devices using smart chip technology. The EMV specifications were developed to address issues with fraud in the magnetic stripe infrastructure and to define a set of requirements to ensure interoperability between smart chip-based payment cards and terminals.

The U.S. is now starting its migration to EMV, with recent announcements by Discover, MasterCard and Visa detailing their roadmaps for issuers, acquirers/processors and merchants. The payment brands' roadmaps were developed to accelerate adoption of both EMV and mobile contactless payments.

For NFC mobile contactless payments, the mobile phone's secure element will be provisioned with the payment brands' EMV application and work with the same EMV contactless point-of-sale readers being put in place globally.

NFC mobile contactless payment transactions between a mobile phone and a POS terminal use the same communications protocol currently used by EMV and U.S.

¹⁰ EMV stands for Europay MasterCard Visa, the three organizations who developed the initial specifications. The EMV specifications are now managed, maintained and enhanced by EMVCo.



Smart Card Alliance

contactless credit and debit cards. This means that consumers can use their NFC-enabled mobile phones for payment at the existing installed base of contactless credit and debit terminals that are based on the EMV standard.

NFC Mobile Contactless Payments: Looking Forward

Globally, the mobile telecommunications industry and the financial payments industry have shown significant commitment to the deployment of NFC mobile contactless payments – not only fielding numerous trials and pilots but also collaborating on the development of the standards, architectures, best practices and security approaches for NFC mobile contactless payments to ensure a secure, interoperable mobile payments infrastructure.¹¹ This broad industry commitment and collaboration make NFC mobile contactless payments unique among the different mobile payments approaches.

NFC offers many benefits to consumers, both to make payments more convenient and to support new, innovative capabilities that deliver value to both the consumer and to merchants. Confidence in the underlying infrastructure and credibility of the industry offerings are critical to consumer adoption. Consumers will benefit from a mobile payments infrastructure that is based on a proven set of standards and architectures, has a strong focus on security, and uses the existing payments infrastructure for transactions.

¹¹ Organizations involved in the development of standards and best practices include: GSMA, ETSI, NFC Forum, Smart Card Alliance, Mobey Forum, GlobalPlatform, EMVCo.



Smart Card Alliance

References and Resources

- EMV Frequently Asked Questions - <http://www.smartcardalliance.org/pages/publications-emv-faq>
- EMV Resources - <http://www.smartcardalliance.org/pages/smart-cards-applications-emv>
- Google Wallet – <http://www.google.com/wallet/>
- Isis – <http://www.paywithisis.com/>
- “MasterCard Introduces U.S. Roadmap to Enable Next Generation of Electronic Payments,” January 30, 2012, <http://www.smartcardalliance.org/articles/2012/01/31/mastercard-introduces-u-s-roadmap-to-enable-next-generation-of-electronic-payments-january-30-2012-framework-to-deliver-enhanced-consumer-experience-in-store-online-at-the-atm-and-with-mobile-phones>
- “The Mobile Payments and NFC Landscape: A U.S. Perspective,” Smart Card Alliance white paper, September 2011, http://www.smartcardalliance.org/resources/pdf/Mobile_Payments_White_Paper_091611.pdf
- NFC Forum – <http://www.nfc-forum.org>
- NFC Trial and Pilots, NFC World, <http://www.nfcworld.com/list-of-nfc-trials-pilots-tests-and-commercial-services-around-the-world/>
- “Security of Proximity Mobile Payments, Smart Card Alliance white paper,” May 2009, http://www.smartcardalliance.org/resources/pdf/Security_of_Proximity_Mobile_Payments.pdf
- NFC Frequently Asked Questions - <http://www.smartcardalliance.org/pages/publications-nfc-frequently-asked-questions>
- NFC Resources - <http://www.smartcardalliance.org/pages/smart-cards-applications-nfc>
- Smart Card Alliance – <http://www.smartcardalliance.org>
- “Visa Announces Plans to Accelerate Chip Migration and Adoption of Mobile Payments,” August 9, 2011 -- <http://www.smartcardalliance.org/articles/2011/08/09/visa-announces-plans-to-accelerate-chip-migration-and-adoption-of-mobile-payments>



191 Clarksville Road
Princeton Junction, New Jersey 08550 (USA)
1.800.556.6828
www.smartcardalliance.org

Smart Card Alliance

Appendix B – Glossary

Chip

An electronic component that performs logic, processing, and/or memory functions.

Contactless payments

Payment transactions that require no physical contact between the consumer's payment device and the physical POS terminal. The consumer holds the contactless card or other device less than 2-4 inches from the merchant POS terminal, and the payment account information is communicated wirelessly via radio frequency (RF).

CTIA

International industry association representing the wireless communications industry.

ECMA International

Industry association founded in 1961 and dedicated to the standardization of information and communication technology and consumer electronics. ECMA is active in defining standards for Near Field Communication.

EMV

Europay MasterCard Visa. Specifications developed by Europay, MasterCard and Visa that define a set of requirements to ensure interoperability between payment chip cards and terminals.

EMVCo

The organization formed in February 1999 by Europay International, MasterCard International, and Visa International to manage, maintain, and enhance the EMV Integrated Circuit Card Specifications for Payment Systems. EMVCo is currently owned by American Express, JCB, MasterCard Worldwide, and Visa, Inc.

ETSI

European Telecommunications Standards Institute. Organization that produces globally-applicable standards for information and communications technologies, including fixed, mobile, radio, converged, broadcast and Internet technologies.

GlobalPlatform

An international, non-profit association, with the mission to establish, maintain and drive adoption of standards to enable an open and interoperable infrastructure for smart cards, devices and systems that simplifies and accelerates development, deployment and management of applications across industries.

GSMA

Industry association that represents the interests of mobile operators worldwide and includes a broad set of companies in the broader mobile ecosystem.

IC

Integrated circuit.



191 Clarksville Road
Princeton Junction, New Jersey 08550 (USA)
1.800.556.6828
www.smartcardalliance.org

Smart Card Alliance

Issuer

The bank that provides a credit card to a cardholder.

IEC

International Electrotechnical Commission. A standards organization for electrical, electronic and related technologies.

ISO

International Organization for Standardization. A non-governmental organization that is a network of national standards institutes of 163 countries, with a central secretariat that coordinates the system.

Mobile contactless payments

A payment to a physical merchant that is initiated from an NFC-enabled mobile phone held in close proximity (within a few centimeters) of the merchant's POS equipment.

Mobile network operator (MNO)

The mobile telecommunications company that has the relationship and mobile phone account with the end user.

Mobile proximity payments

Mobile payment transaction in which a consumer uses a phone to pay for goods or services at a physical POS.

Mobile remote payments

Mobile payment transactions in which consumers use a smartphone or mobile phone to make purchases without interacting with a physical POS.

Mobile wallet

A software application that is loaded onto a mobile phone to manage payments made from the mobile phone. A mobile wallet application can also hold and control a number of other applications (for example, payment and loyalty), much as a physical wallet holds a collection of physical cards.

Near Field Communication (NFC)

A standards-based wireless communication technology that allows data to be exchanged between devices that are a few centimeters apart. NFC-enabled mobile phones incorporate a smart chip (called a *secure element*) that allows the phone to store the payment application and consumer account information securely and use the information as a virtual payment card. NFC payment transactions between a mobile phone and a POS terminal use the standard ISO/IEC 14443 communication protocol currently used by EMV and U.S. contactless credit and debit cards.

NFC Forum

Industry association that was formed to advance the use of Near Field Communication technology by developing specifications, ensuring interoperability among devices and services, and educating the market about NFC technology.



191 Clarksville Road
Princeton Junction, New Jersey 08550 (USA)
1.800.556.6828
www.smartcardalliance.org

Smart Card Alliance

OTA (Over-the-air)

The possibility to send data to and receive data from a mobile device in a distributed environment. In GSM networks, OTA can use a data connection or SMS.

Personalization

The process of incorporating the unique personal data for a user into a generic device or card.

PIN (Personal identification number)

The numeric code associated with a payment account or card that adds a second factor of authentication to the identity verification process.

POS (Point-of-sale)

The merchant's physical location where the payment transaction takes place. This term is also used to describe the equipment used by the merchant to complete the payment transaction.

Reader

Any device that transmits data or assists in data transmission between a card, token, or other device and a host computer or database.

Smart card

A device that includes an embedded secure integrated circuit that can be either a secure microcontroller or equivalent intelligence with internal memory or a secure memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless radio frequency interface. With an embedded microcontroller, smart cards have the unique ability to securely store large amounts of data, carry out their own on-card functions (e.g., encryption and mutual authentication), and interact intelligently with a smart card reader. Smart card technology conforms to international standards (ISO/IEC 7816 and ISO/IEC 14443) and is available in a variety of form factors, including plastic cards, subscriber identification modules (SIMs) used in GSM mobile phones, and USB-based tokens.

Smart chip

The secure integrated circuit that is used in smart cards and other form factors. Smart chips are embedded in plastic cards, subscriber identification modules (SIMs) and secure elements used in mobile phones, and USB-based tokens.

Secure element (SE)

The component in a mobile phone that provides security and confidentiality. A secure element can reside on the SIM, in a dedicated chip on a phone's motherboard (embedded secure element), or as an external accessory. The secure element is a smart card chip that contains a dedicated microprocessor with an operating system, memory, an application environment, and security protocols. It is used to store and execute sensitive applications on a mobile device.

Trusted service manager (TSM)


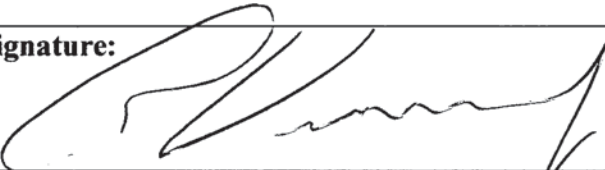
A neutral third party who provides a single integration point with mobile operators for financial institutions, and retailers who want to provide a payment, ticketing, loyalty or other NFC application to their customers with NFC-enabled phones.



United States House of Representatives
Committee on Financial Services

“TRUTH IN TESTIMONY” DISCLOSURE FORM

Clause 2(g) of rule XI of the Rules of the House of Representatives and the Rules of the Committee on Financial Services require the disclosure of the following information. A copy of this form should be attached to your written testimony.

1. Name: Randy Vanderhoof	2. Organization or organizations you are representing: Smart Card Alliance
3. Business Address and telephone number: 	
4. Have <u>you</u> received any Federal grants or contracts (including any subgrants and subcontracts) since October 1, 2008 related to the subject on which you have been invited to testify? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	5. Have any of the <u>organizations you are representing</u> received any Federal grants or contracts (including any subgrants and subcontracts) since October 1, 2008 related to the subject on which you have been invited to testify? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
6. If you answered .yes. to either item 4 or 5, please list the source and amount of each grant or contract, and indicate whether the recipient of such grant was you or the organization(s) you are representing. You may list additional grants or contracts on additional sheets.	
7. Signature: 	

Please attach a copy of this form to your written testimony.