THE FUTURE OF MONEY: HOW MOBILE PAYMENTS COULD CHANGE FINANCIAL SERVICES

HEARING

BEFORE THE

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

MARCH 22, 2012

Printed for the use of the Committee on Financial Services

Serial No. 112–110

U.S. GOVERNMENT PRINTING OFFICE

75–082 PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

HOUSE COMMITTEE ON FINANCIAL SERVICES

SPENCER BACHUS, Alabama, *Chairman*

JEB HENSARLING, Texas, *Vice Chairman*
PETER T. KING, New York
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
RON PAUL, Texas
DONALD A. MANZULLO, Illinois
WALTER B. JONES, North Carolina
JUDY BIGGERT, Illinois
GARY G. MILLER, California
SHELLEY MOORE CAPITO, West Virginia
SCOTT GARRETT, New Jersey
RANDY NEUGEBAUER, Texas
PATRICK T. MCHENRY, North Carolina
JOHN CAMPBELL, California
MICHELE BACHMANN, Minnesota
THADDEUS G. McCOTTER, Michigan
KEVIN McCARTHY, California
STEVAN PEARCE, New Mexico
BILL POSEY, Florida
MICHAEL G. FITZPATRICK, Pennsylvania
LYNN A. WESTMORELAND, Georgia
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
SEAN P. DUFFY, Wisconsin
NAN A. S. HAYWORTH, New York
JAMES B. RENACCI, Ohio
ROBERT HURT, Virginia
ROBERT J. DOLD, Illinois
DAVID SCHWEIKERT, Arizona
MICHAEL G. GRIMM, New York
FRANCISCO "QUICO" CANSECO, Texas
STEVE STIVERS, Ohio
STEPHEN LEE FINCHER, Tennessee

BARNEY FRANK, Massachusetts, *Ranking Member*
MAXINE WATERS, California
CAROLYN B. MALONEY, New York
LUIS V. GUTIERREZ, Illinois
NYDIA M. VELAZQUEZ, New York
MELVIN L. WATT, North Carolina
GARY L. ACKERMAN, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
MICHAEL E. CAPUANO, Massachusetts
RUBÉN HINOJOSA, Texas
WM. LACY CLAY, Missouri
CAROLYN MCCARTHY, New York
JOE BACA, California
STEPHEN F. LYNCH, Massachusetts
BRAD MILLER, North Carolina
DAVID SCOTT, Georgia
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
GWEN MOORE, Wisconsin
KEITH ELLISON, Minnesota
ED PERLMUTTER, Colorado
JOE DONNELLY, Indiana
ANDRÉ CARSON, Indiana
JAMES A. HIMES, Connecticut
GARY C. PETERS, Michigan
JOHN C. CARNEY, JR., Delaware

JAMES H. CLINGER, *Staff Director and Chief Counsel*

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

SHELLEY MOORE CAPITO, West Virginia, *Chairman*

JAMES B. RENACCI, Ohio, *Vice Chairman*
EDWARD R. ROYCE, California
DONALD A. MANZULLO, Illinois
WALTER B. JONES, North Carolina
JEB HENSARLING, Texas
PATRICK T. McHENRY, North Carolina
THADDEUS G. McCOTTER, Michigan
KEVIN McCARTHY, California
STEVAN PEARCE, New Mexico
LYNN A. WESTMORELAND, Georgia
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
SEAN P. DUFFY, Wisconsin
FRANCISCO "QUICO" CANSECO, Texas
MICHAEL G. GRIMM, New York
STEPHEN LEE FINCHER, Tennessee

CAROLYN B. MALONEY, New York,
Ranking Member
LUIS V. GUTIERREZ, Illinois
MELVIN L. WATT, North Carolina
GARY L. ACKERMAN, New York
RUBÉN HINOJOSA, Texas
CAROLYN McCARTHY, New York
JOE BACA, California
BRAD MILLER, North Carolina
DAVID SCOTT, Georgia
NYDIA M. VELÁZQUEZ, New York
GREGORY W. MEEKS, New York
STEPHEN F. LYNCH, Massachusetts
JOHN C. CARNEY, JR., Delaware

CONTENTS

WITNESSES

THURSDAY, MARCH 22, 2012

APPENDIX

THE FUTURE OF MONEY: HOW MOBILE PAYMENTS COULD CHANGE FINANCIAL SERVICES

Thursday, March 22, 2012

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS
AND CONSUMER CREDIT,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The subcommittee met, pursuant to notice, at 10:02 a.m., in room 2128, Rayburn House Office Building, Hon. Shelley Moore Capito [chairwoman of the subcommittee] presiding.

Members present: Representatives Capito, Renacci, Luetkemeyer, Huizenga, Grimm; Maloney, McCarthy of New York, Scott, and Carney.

Chairwoman CAPITO. This hearing will come to order.

I appreciate the witnesses being here. We are expecting a series of votes as early as 11:30, and if we are unable to complete the hearing before the votes, we will return after votes are completed.

But we meet today to begin what I think is an exciting and important task, which is making sure our financial system and its regulatory structure are prepared to enter the new world of mobile payments.

You see a lot of press about mobile banking; certainly a lot of advertising on mobile banking. And without saying too much about my general age area, this is age-specific in some ways considering my mother has never used an ATM, but she does pump her own gas.

I know what my children, who in their 20s, are going to be doing in terms of how they bank. And this is what I think is the relevance—why I am extremely interested in this as we move through this panel.

While most people believe that making a mobile payment involves waving a smartphone at a cash register, and it may be, there are a lot more ways to exchange values.

Contactless cards and short e-mail messages giving instructions to transfer value represent other form of mobile payments. The whole field offers the possibility of faster and cheaper transfers of value, oftentimes with the promise of enhanced security that surpasses what is possible today.

We are, I think, on a precipice of some fundamental change in the way money is exchanged between consumers and businesses.

And that is why I am interested and I wanted to have this hearing on the future of money.

While some aspects of mobile payments have been with us for a while, and some business models are already developed, other aspects of mobile payments are in the beginning stages of pilot programs. Either way, there is a lot for Congress, banks, regulators, retailers, and customers to learn.

Most importantly, we want to make sure these payments are safe and secure; at least as safe as using cash, checks or credit cards, and hopefully even more so. Bringing the strength of high-powered computers to bear on account safety could allow us to erect layers of security that help foil the hackers who lie in wait on the Internet today, stealing millions of identities—and we have looked into this in our subcommittee as well—and billions of dollars annually.

After all, the smartphone that was essentially nonexistent less than 6 years ago, is said to be far more powerful than the large supercomputers of the 1980s, or certainly of those of us who went to college in the 1970s and took computer science and we had those stacks of cards that we had to feed into the computer and stay in the computer room all night to make sure they went through.

Today's hearing is an introduction to mobile payments, the first I am aware of to be held by Congress. We have five expert witnesses who can discuss broadly the state of the mobile payment industry and where and how fast they see it developing.

Among them is Richard Oliver. Until he retired last year, he was the Federal Reserve's top mobile payments expert and the principal author of the Fed's widely praised White Paper on the subject. We also have experts from the issuer side, from the standards sides of mobile payments, and a consumer specialist.

So I look forward to hearing everybody's testimony and I would now like to recognize the ranking member from New York, Mrs. Maloney, for the purpose of making an opening statement.

Mrs. MALONEY. First of all, I would like to thank Chairwoman Capito for holding this hearing, one in a series on the future of mobile payments in our financial system.

And thank you to all the panelists for joining us this morning. I believe this hearing will serve as a great first step and learning session on this rapidly evolving technology. I feel that this is another example of American exceptionalism, of coming up with an innovative idea, an efficient idea that keeps America moving forward and employing more people, becoming more efficient and making us an even stronger country.

I am excited about this idea and I really look forward to hearing all of your testimony.

Mobile payments in the United States are expected to generate $215 billion by the year 2015. Forty-three million adults in this country use alternative financial services as a form of banking. And as this technology continues to move forward, it creates innovative and exciting opportunities for everyday citizens at home and at work.

The possibilities are truly endless. We are seeing what technology can do for consumers and businesses as mobile technology opens the door to an entirely new method of financial interaction.

Mobile payments, payments made by electronic means, effectively replace cash, checks, and traditional credit cards. This evolving form of financial exchange can provide consumers with greater purchasing power; allow merchants to market their goods more efficiently; and help create a truly mobile, electronic, and innovative society.

Mobile payments can involve text messages that transfer funds from one person to another or to a financial institution, as experienced in the successful program to funnel aid to earthquake victims in Haiti. I was truly stunned at how successful this program was. They had on every taxicab, "Get on your mobile phone and text $5 to the earthquake victims." And that successful effort led to $5 million in $10 donations from Americans throughout our great country through their cellphone carriers.

This happened—truly outstanding possibilities for this new form of payment. And mobile payment technology can allow consumers to wave their phones at checkouts and even direct those charges to prepaid phone deposits and phone bills. I love it. It just gets better and better. We wouldn't lose all our papers all the time if we had this.

And as mobile phones become more prevalent, and as the number of methods of making payments increase, it is important to look at the hurdles facing its implementation.

How much will the adoption of mobile payments cost merchants as they purchase and install readers for their technology? How protected are consumers? Can hackers steal their data out of the air? What is the level of disclosure that will be provided to our consumers—greater regulatory clarity for this market? Consumers want payments that are convenient and inexpensive.

But we must make sure that security is not abandoned for the sake of this new technology. It may be years before this technology fully becomes a reality for the majority of people the way debit cards have. However, I am happy that we are discussing this important issue at the ground level. I congratulate the chairwoman for calling this important hearing. I look forward to your testimony and I welcome everybody.

Chairwoman CAPITO. Thank you.

Mr. Renacci, for 1 minute, for an opening statement.

Mr. RENACCI. Thank you Madam Chairwoman.

This is an exciting time in the payments industry. Over the last several years, innovative companies have invested huge amounts of capital and manhours to lay the groundwork for many of the methods we are discussing here today.

New innovations in smartphones and mobile payments are bringing consumers greater convenience and a better buying experience, while also increasing the security of payment transactions. While I am interested to learn about these new products and services here today, I also want to hear what we in Congress can do to make sure that these innovations progress in a safe and prosperous manner.

We must encourage a free market where innovators can realize the benefits of their investments and consumers can benefit from lower costs and safer products. I look forward to hearing your testimony today.

I yield back the remainder of my time.

Chairwoman CAPITO. Thank you.

I don't think Mr. Grimm wanted to make an opening statement, so we will go ahead and go directly to the testimony.

I want to recognize the witnesses for the purpose of making a 5-minute statement, and then we will go to the question-and-answer period.

As I mentioned in my opening statement, we are really lucky and pleased to have Mr. Richard Oliver here. He is the co-author of "Mobile Payments in the United States: Mapping Out the Road Ahead," which was published by the Federal Reserve Bank of Atlanta.

Welcome, Mr. Oliver.

STATEMENT OF RICHARD R. OLIVER, PAYMENTS CONSULTANT/RETIRED EXECUTIVE VICE PRESIDENT, THE FEDERAL RESERVE BANK OF ATLANTA, AND CO-AUTHOR OF "MOBILE PAYMENTS IN THE UNITED STATES: MAPPING OUT THE ROAD AHEAD"

Mr. OLIVER. Thank you very much.

And let me start by thanking the committee and the subcommittee for the opportunity to come and share information with you about the mobile payments environment while it is still very early in its evolution.

In 2010 payments research teams from the Federal Reserve Banks of Atlanta and Boston collaborated to conduct an assessment of the state of and potential for deployment of mobile payment options in the United States. Our interests were to determine the impact of mobile payments on existing payments businesses and to isolate potential risks to consumers and businesses who might choose to use mobile payment options.

To conduct the assessment, we invited most of the major players from the mobile payments industry to discuss with us on a voluntary basis the opportunities, barriers, and challenges associated with implementing a successful mobile payments environment in this country.

The attendees included major card brands, wireless operators, financial institutions, industry trade groups, retailers, and many other participants.

Please note that this effort was not directed at mobile banking, which is the use of your mobile phone to access online banking functions. It was directed at actually exchanging value at the point of sale utilizing your phone.

Over the course of what turned out to be seven meetings during 2010 and 2011, we not only gained great insight into the evolution of mobile payments in the country, but the group helped us isolate a series of key factors that they collectively felt should be met to ensure a safe implementation of mobile payments in this country. And my purpose here today is to share those with you.

The first was that the proposed environment should be best defined as an open wallet. That is, a wallet that would allow complete access by all persons using all credentials they might want to use as opposed to proprietary initiatives that might limit the amount of instruments available for use by a consumer.

Second, the mobile infrastructure would likely be based on near-field communications technology, resident and mobile devices, and in retail point-of-sale terminals. This technology is now becoming common in other countries and would allow users to tap their phones and institute a purchase.

Third, existing, well-protected clearing and settlement rails would likely be the way that value would be exchanged. That is through the debit card, credit card, and prepaid and automated clearinghouse networks to be used for clearing and settlement between parties.

Fourth, some form of enhanced security such as dynamic data authorization should be used to deter counterfeiting and I.D. theft at the point of sale. This technology is already resident in chip and pin cards being used throughout the world.

Fifth, common standards should be designed, developed, certified, and implemented throughout the industry to ensure interoperability, efficiency, and ease of use by consumers and businesses.

Sixth, the regulatory oversight regimen for mobiles should be made clear early on and participants should be involved in these compliance activities.

Bank and nonbank regulators such as the FCC, the FTC, and the new Consumer Financial Protection Bureau should collaborate early on to define the regulatory environment for all the participants.

Seventh, entities such as a trusted service manager that exist in the card world today should oversee the provision of the interoperable and shared security elements in the phone.

The group also recognized the possible need over time for some entity to serve as a coordinating party to keep the very diverse participants on track and working together and possibly to create a roadmap for the future to allow the participants to understand how to minimize their long-term investments in the technology that is necessary.

However, the majority of the group at the time felt it was too early in the process to do this and the completion of early pilots and tests would better inform such work.

All of this information and more was captured in the White Paper that you alluded to, which was authorized by the participants and cooperatively authored by the two Reserve Banks.

It is available on Reserve Bank Web sites. It has been well-vetted at conferences and trade press over the past year, and was shared with all of the Federal regulators and law enforcement agencies at a session we held in the first half of last year, at which my colleague from Boston and I presented.

As the work proceeded, most of the participants have decided to participate in a number of pilots and test situations going on that should better test the validity of these aforementioned principles and pave the way for more widespread deployment.

In closing, the work group continues to meet on issues of common interest such as data security. But they have been outspoken recently about the need to educate and inform business, government and consumers about the mobile environment.

We view this hearing as a great first step in this process and appreciate the opportunity to participate. Thank you.

[The prepared statement of Mr. Oliver can be found on page 55 of the appendix.]

Chairwoman CAPITO. Thank you very much.

Our next witness is Mr. Troy Leach, chief technology officer, PCI Security Standards Council. Welcome.

STATEMENT OF TROY LEACH, CHIEF TECHNOLOGY OFFICER, PCI SECURITY STANDARDS COUNCIL, LLC

Mr. LEACH. Chairwoman Capito, Ranking Member Maloney, and members of the subcommittee, thank you for the opportunity to testify on the important topic of mobile payment security.

My name is Troy Leach. I am the chief technology officer for the Payment Card Industry Security Standards Council, also known as the PCI Council.

Formed in 2006 by the major payment card brands, the Council guides the development of open industry standards to protect payment information.

More than 600 companies worldwide participate in the Council's work for many different industries and backgrounds, including a number of the leading players in the mobile space, including a number of people who will be spoken about later today.

So it is exciting for us to be here today representing these members, from restaurants to banks to airlines to technology vendors, who are eager to realize the benefit of mobile payment acceptance in the most secure way possible.

The PCI standards are a strong industry framework for protecting payment data. And it is this framework that we are applying to mobile payment acceptance space.

Mobile technology is exciting and dynamic with a potential to change the way we accept payments not only in the United States, but also around the world. The benefits could be significant. However, both consumers and merchants want to know that using mobile technology for payment is just as safe as using a traditional form of payment.

From our perspective at the council, making it secure is our priority. For traditional payment card security, for the Council, we have focused on people, process and technology.

The mobile payment environment is very complex, more so than the traditional payment card scenario. Our goal is to work with the industry to provide security across that spectrum.

Let me also clarify the Council's focus. There are two aspects to mobile payments: initiation; and acceptance. The first is when a consumer is using a phone in place of a payment card to make a purchase. That is initiation. And the other is where a mobile device, perhaps even the same mobile phone, is being used by a merchant to accept payment cards.

There are a number of groups, including some of my fellow panelists, working on the first aspect with the aim to protect consumer's payment data.

The Council's security efforts have been focused on the second area of payment acceptance, specifically of securing the use of mobile devices as a point-of-sale acceptance tool.

Our first step has been to make sure that merchants can use mobile technology to accept payments safely and to protect their cus-

tomers' information. PCI standards already apply to mobile acceptance today, addressing the security of mobile devices, of mobile applications, and the environments in which they operate.

Expanding on these standards, we have published security requirements that make it possible for merchants to use plug-in devices with mobile phones to swipe payment card data.

We have also put out guidance on developing mobile payment acceptance applications to help merchants process these payments securely. And we will be releasing additional best practices later this year on securing mobile payment transactions.

As payment security is a shared responsibility, all parties in the payment chain must work together in this effort. The Council is concerned with making sure that these parties are validated in the products and services that they provide. And moving forward, we will explore this area even further.

Lastly, great work is being done through the advancement of technologies in payment. Technologies are emerging that have the ability to eliminate card data from potentially insecure mobile environments.

The Council has already harnessed some of these technologies to address this dynamic environment and we will continue to assess and develop standards and guidance around them moving forward.

In closing, mobile technology offers exciting potential to that payment space. To help realize this securely, the Council will work with its global stakeholders to develop industry standards and the resources necessary for the protection of cardholder data across all payment channels and the reduction of fraud for consumers and businesses globally.

Thank you. I look forward to your questions.

[The prepared statement of Mr. Leach can be found on page 30 of the appendix.]

Chairwoman CAPITO. Thank you very much.

Our next witness is Mr. Ed McLaughlin, chief emerging payments officer, MasterCard Worldwide. Welcome.

STATEMENT OF ED MCLAUGHLIN, CHIEF EMERGING PAYMENTS OFFICER, MASTERCARD WORLDWIDE

Mr. MCLAUGHLIN. Thank you, and good morning, Chairwoman Capito, Ranking Member Maloney, and members of the subcommittee.

My name is Ed McLaughlin. I am the chief emerging payments officer at MasterCard Worldwide based in Purchase, New York. It is my pleasure to appear before you today and discuss developments in mobile payment.

MasterCard is a leader in the transformation of mobile phones and to secure payment devices and a champion of global mobile payment standards. We appreciate the opportunity to be here today to share our perspective on how mobile payments are developing and benefiting consumers and businesses.

As mobile payments continue to evolve, we need to constantly focus on two goals. First, we must strive to make paying for something as simple and as compelling as possible for every participant in the payments chain.

Second, we must provide the highest level of security to consumers, to merchants, and to our financial institution customers. At MasterCard, we invest heavily in the technologies that make both of these goals possible.

Now, as you might expect, mobile devices are bringing changes to the way people interact and also how they want to transact. For example, the acceptance of card-based payments through the use of handheld devices is opening up channels of transactions for entrepreneurs that were not possible just a few years ago.

Smartphones also provide a platform for the delivery of new applications that are transforming the in-store shopping experience for consumers. For merchants, smartphones provide a convenient channel to engage consumers at multiple levels such as through an Internet storefront or social media account.

Smartphones themselves are also becoming payment devices through the adoption of near field communication, or NFC, technology. MasterCard's PayPass, our Tap & Go product, is at the forefront of this space. And by 2016, it is anticipated that the majority of smartphones will support this technology.

So why are the new uses for mobile phones so important? Because they provide convenience and promote financial inclusion in a very secure environment.

Unlike the simple plastic card that has been around for decades, smartphones provide an intelligent device right in the consumer's hands that the consumer can use to interact with financial service providers and merchants in ways that were never before possible.

Also, when you look at the 85 percent of transactions that are still being funded through cash and check, it is clear that smartphone technology provides an unprecedented opportunity to accelerate the transition to safe and secure electronic payments.

By enhancing the ways that people connect to our network, we are able to deliver new services to benefit consumers and to reach a large number of consumers who are currently outside the financial mainstream.

For example, payment card solutions like prepaid cards, coupled with mobile technology, can unlock the global commerce grid to consumers who do not currently have access to mainstream financial services.

So at MasterCard, we have invested substantial financial resources and human capital in developing the technology necessary for our part in the mobile payments ecosystem.

Each day, we strive to make payments simple for all participants in the payment chain while providing those highest levels of security. For example, this is why we applied MasterCard's zero liability protections for consumers to these new payment technologies, including mobile-based payments.

In addition, we have recently announced a program to transition MasterCard-branded payment products in the United States to the EMV standard. The EMV standard is a global standard for debit and credit payments based on chip technology, the objective of which is to ensure interoperability globally and acceptance of payment cards on a worldwide basis.

The adoption of EMV-compliant payments in the United States will help provide additional layers of protection for consumers at the points of interaction.

MasterCard is extremely proud of the role we play in advancing commerce through new technologies. The mobile phone and many other smart handheld devices are transforming the way we conduct our everyday lives, and hold significant promise for providing new value to consumers and businesses, particularly in the delivery of financial services.

Again, I appreciate the opportunity to appear before you today, and when we get to it, I will be glad to answer any questions you may have.

Thank you.

[The prepared statement of Mr. McLaughlin can be found on page 43 of the appendix.]

Chairwoman CAPITO. Our next witness is Mr. Randy Vanderhoof, executive director, Smart Card Alliance.

Welcome.

STATEMENT OF RANDY VANDERHOOF, EXECUTIVE DIRECTOR, SMART CARD ALLIANCE

Mr. VANDERHOOF. Thank you.

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 nonprofit organization that provides education and a collaborative open forum among leaders in various industries, including mobile payments.

We applaud the subcommittee's interest in making mobile payments safe, flexible, and resilient with the appropriate legal, regulatory, and security frameworks.

Mobile devices can be used to facilitate the payment process in many ways. I am going to focus my remarks on the use of a payment-application-enabled mobile phone that can be used to pay at a physical merchant location as an alternative to paying with a plastic 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 the type of mobile payments that I am here to talk about today is built on already-established legal, regulatory, and security frameworks in both the payment and the wireless telecom industries.

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 enables secure mobile payment at physical merchant locations.

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 covered by existing laws and regulations.

Second, the security and reliability of this approach are grounded in global standards, established certification processes, and in industry best practices that are the culmination of nearly 20 years of work in applying smartcard chip technology to protect payment accounts and mobile phone subscribers.

Multiple international standards have been developed for NFC mobile payment, and are supported by the mobile industry and endorsed by the payment industry. In addition, new and existing safeguards are used with mobile payment devices to add many layers of protection for consumer account information and transactions.

For example, 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 customer's mobile operator. The NFC-enabled phone is provisioned with a digital payment credential issued by a bank and stored in a new, specially designed, secure memory location in the phone.

The credential is transmitted to a merchant's NFC-enabled payment terminal by short-range wireless communications. The authorization and settlement processes are the same for those used when the consumer pays with a traditional credit or debit card.

Market development involving many of America's largest and most trusted companies is well under way. One example is Isis, a new mobile carrier joint venture between AT&T, Verizon Wireless, and T-Mobile using the NFC mobile contactless payment technology we are discussing today. Isis will license payments provided by 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 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 purchases and coupon offers.

NFC payment-embedded and mobile phones won't be the only form of mobile payment. There are new mobile technologies being tested other than NFC that are promising yet still unproven. NFC offers value to both consumers and merchants. In addition to value, consumers' confidence is in the underlying infrastructure, and the credibility of industry offerings are critical to its adoption.

Consumers will benefit from and trust in a mobile payments infrastructure that has a strong focus on security and uses the existing payments infrastructure for transactions.

Mobile phones represent a fertile landscape for new ways consumers can transact with retailers, financial institutions, application stores, and each other. Mobile payments innovation is going to continue to evolve, as more people upgrade to smartphones and learn about the new services they hold in the palm of their hand.

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

The Smart Card Alliance would like to thank the subcommittee once again for holding this important and forward-looking hearing. We greatly appreciate the opportunity to present information that assists in the setting of legal, regulatory, and security frameworks necessary to implement safe, flexible, and resilient mobile financial products.

Thank you.

[The prepared statement of Mr. Vanderhoof can be found on page 58 of the appendix.]

Chairwoman CAPITO. Thank you.

And our final witness is Ms. Suzanne Martindale, staff attorney with the Consumers Union.

Welcome.

STATEMENT OF SUZANNE MARTINDALE, STAFF ATTORNEY, CONSUMERS UNION OF U.S., INC.

Ms. MARTINDALE. Madam Chairwoman, Ranking Member Maloney, and members of the subcommittee, thank you very much for the opportunity to testify today on behalf of Consumers Union, the advocacy policy arm of Consumer Reports.

Mobile payments allow consumers to buy products or transfer money with a mobile device. The market includes a range of different technologies and many ways to fund the transactions. The U.S. mobile payments market is still developing and it remains unclear which trends will prevail.

It is too soon to know which consumers will benefit most from the industry's growth, or inversely, be most vulnerable to risk. However, policymakers can make a few simple fixes to ensure that all mobile payments are safe.

The mobile payments market is, in a word, complex. There are multiple ways to initiate payments. Some services involve sending a text message or using an application downloaded to the device. Others employ a chip embedded in the hardware which the consumer waves at a contactless reader.

Furthermore, multiple parties are involved in completing the transaction. You have consumers, merchants, third-party processors, wireless carriers, and financial institutions, all in the same ecosystem. With so many players involved, the risk of confusion for the consumer increases, should something go wrong.

Who is responsible for fixing the problem? If the different parties all point fingers at each other, the consumer may be out of luck.

Despite these challenges, mobile payments in the United States are projected to gross $214 billion by 2015, in part due to their potential to provide speed and convenience for consumers and merchants. Some merchants are interested in the technology because mobile payment service providers may charge lower processing fees than traditional networks at the point of sale.

Mobile payment technologies also have the potential to serve new audiences. This may appeal to young, tech-savvy consumers, as well as consumers who go outside the traditional banking system for financial services. For unbanked or underbanked consumers, as we call them, mobile payments may provide increased access to financial services.

Low-income households and households of color, in particular, are more likely to be unbanked or underbanked. And according to a recent Pew study, these same households are more likely to adopt cellphones and smartphones compared to the general population. This presents an opportunity for mobile payment technologies to penetrate these markets. However, these same markets may be vulnerable to risk without adequate safeguards.

Internationally, mobile payments have garnered attention for helping consumers in developing countries gain access to financial services. An estimated 5 billion consumers worldwide have a mobile phone, but only 1.5 billion have a bank account.

In Kenya, where more consumers have cellphones than have bank accounts, Safaricoms' popular M–PESA service enables consumers to manage transactions entirely through their mobile phones, not smartphones, just regular cellphones. M–PESA customers can deposit or withdraw cash and send money through a network of ATMs and agents, and they can buy goods and services with their mobile phone, all without needing a bank account.

However, U.S. consumers have been slow to adopt mobile payments for several reasons. Some mobile payments systems remain limited in scope and availability. For example, the new Google Wallet uses an NFC, or near field communication, chip embedded in the mobile device, which the consumer waves at a contactless reader. However, Google Wallet is currently only available to Sprint customers with a particular phone, the Nexus S smartphone.

Another mobile payment system, Bling Nation, uses a sticker with an embedded chip that the consumer affixes to the device and waves at a reader. However, Bling Nation is still available only through pilot programs in Palo Alto, Chicago, and Austin.

Furthermore, market research indicates that consumers have concerns about security of their financial information. In a survey released last week, the Federal Reserve found that over 40 percent of consumers still cite security concerns as a reason for not adopting mobile payments.

Finally, not all ways to pay with a mobile device are created equal when it comes to consumer protection. Although consumers may not be aware of it, U.S. payments law is fragmented. The level of protections against unauthorized transactions and errors varies, depending on whether a consumer links payment to a credit card, a debit card, a prepaid card, a bank account, a prepaid phone deposit, or a phone bill.

Traditional credit and debit cards have mandatory protections under existing law; however, prepaid cards do not. Mobile payment links to a prepaid phone deposit or a phone bill are especially problematic, because they do not neatly fit into the existing legal categories.

Wireless carriers may provide voluntary protections, but they are typically not disclosed in customer contracts. The different ways to pay by mobile device, and the varying protections that apply to each, create the potential for confusion when a consumer is faced with a transaction gone wrong.

Consumers need to know where to complain and how to get their money back, in case of errors or unauthorized use. Consumers cannot afford to lose precious funds due to inadequate protections. And

for low- and moderate-income consumers, this loss could be especially acute.

Until U.S. payments law is updated to provide clear, guaranteed protections for all payment methods, consumers may be at risk when using mobile payments technology. Nevertheless, a few simple fixes could close the gaps in protection and provide clarity to the industry.

The Consumer Financial Protection Bureau is in a unique position to address mobile payments, because it has jurisdiction over payment service providers and can clarify regulations implementing Federal consumer financial laws.

Congress and other Federal agencies also have a very important role to play in establishing some sensible rules for the road that protect consumers and foster innovation.

Thank you again for the opportunity to testify. I welcome your questions.

[The prepared statement of Ms. Martindale can be found on page 39 of the appendix.]

Chairwoman CAPITO. Thank you.

I want to thank all of you. And I will begin with the questions.

First of all, Mr. Oliver, just so I understand, I am starting here with the basics. You mentioned "open wallet." Can you just explain what an "open wallet" is?

Mr. OLIVER. The concept of the "open wallet" is that it would operate on the phone the same way it does in your current wallet. And you can select on that phone any payment instrument you choose from any provider and execute a payment using standard technology without having to do something terribly different from paying an instrument to another.

Chairwoman CAPITO. So you could pay out of your bank account on your card?

Mr. OLIVER. Out of your bank account, or any card you may have in your wallet. Competing cards, prepaid cards, what-have-you.

Chairwoman CAPITO. Right. Okay.

My understanding, and I am sort of throwing this out to anybody who knows this—is that Europe has been much further ahead than we are on this technology. They have the chip and PIN cards, I guess they are using in Europe? And there is some thought that this NFC chip would sort of leapfrog that technology.

Why do you think it has caught on there and it hasn't caught on here? And do you in fact think that this will leapfrog their technology? I imagine it is going to catch on like wildfire once it gets going in a more robust fashion.

Does anybody know why the European model is further ahead than we are on this technology?

Mr. MCLAUGHLIN. Let me open. When you look at markets and how they evolve, it usually starts at the baseline conditions. The United States benefited from having the best telecom infrastructure in the world at the times they were looking at. So there are requirements in Europe to be able to handle things like offline transactions; to put more intelligence into the transactions themselves to purely compensate for the telecoms infrastructure that were there. So that led to a set of investments in EMV and underlying security technology.

We have seen that now cascade in markets around the world—Canada, Mexico, and other markets are moving towards endorsing that.

So in the United States, we now see it as absolutely time for us to move from static, plastic-based credentials to dynamic protections that can be generated using EMV and chip technology. In many ways, we took a plastic card and we put a chip on the card. We are now taking the chip off the card and putting it into the phone.

Chairwoman CAPITO. In the phone.

Mr. MCLAUGHLIN. It is also essential, though, as we work on this, that we continue to maintain that worldwide interoperability so consumers know that anywhere that they can go, they can get the same security around their payment products.

Chairwoman CAPITO. I agree with that.

The question I have on—I think all of you have mentioned the contactless reader which would be at the vendor site, the retailer site. I represent a rural area and there is always a question of cost for the retailer. How expensive are these devices? Are people investing in them? Somebody mentioned 20 retailers who are involved in this, the larger retailers.

How do you see this in terms of the retailer investment? I know when we changed the interchange, there was a big hue and cry from the retailer to the different readers and so does anybody have any kind of statement on that?

Mr. VANDERHOOF. I would like to begin by saying that when the U.S. brands—particularly Visa, MasterCard and Discover—announced that they were moving towards the EMV chip strategy within the last year, an important distinction that they included in that road map was that they were going to incorporate both contact and contactless technology as a part of that in order to be able to embrace the mobile contactless technologies that we are talking about here today.

From a merchant perspective, they now have a very clear and distinct path forward in terms of what will be the technology platform not only to accept their existing payment cards that consumers have today, the new and emerging EMV chip cards that are coming, but also the mobile NFC payments technology.

The advantage for the merchants now is that when they do make that decision to upgrade their acceptance infrastructure in their stores, they can purchase one device that is going to support the legacy card technology that is in the market today, the evolving new chip contact card technology that is coming and the NFC mobile technology in the phone. So they will make one investment supporting three of their primary methods of payment.

Chairwoman CAPITO. Is that technology available right now?

Mr. VANDERHOOF. It is not only available, but also the manufacturers of those devices have now totally upgraded their equipment to be able to absorb these new technologies so that the same devices that they would purchase 5 years ago didn't have—

Chairwoman CAPITO. Right. I understand. Yes. I understand.

I have just a couple of seconds because I think the security issue is something that we want to delve deeply into.

I think Ms. Martindale brought out a great question, "If something goes wrong, how are you going to track back as a consumer to figure out how you are going to right that wrong?"

And the other thing that Mr. McLaughlin mentioned that I think we should be looking at here is talking with the regulators about—as you mentioned, this is regulated as a card. But then, Ms. Martindale brought up some exceptions to it that I think are significant with the evolution of different types of cards. And I think that is something we need to keep our eye on.

I am now going to yield to Mrs. Maloney for 5 minutes for questions.

Mrs. MALONEY. I want to thank you, Mr. Oliver. In your statement, you said we should come out with common standards that would help us more efficiently move this forward. Where do you see these common standards coming from? Who is going to pull them together? The industry or whatever?

Mr. OLIVER. Yes, these are best and usually done by industries. And Mr. Vanderhoof made several comments about the efforts of the Smart Card Alliance and others. There are forums in Europe as well as international standard forums such as ISO that generate these types of standards and allow people to adopt them.

It is a critical issue in interoperability and really the key to the earlier question about an open wallet; that you would have the same experience no matter what you did. So there are organizations collaboratively participated in that would generate these.

Mrs. MALONEY. That is great news because on 9/11, one of our biggest challenges was that the phones from the police couldn't interact with the phones from the fire department. And if they could have, it could have saved lives. So making that commonsense step forward would be important.

Many of you talked about how this would allow more access for the unbanked and those who don't have access to banking. Would someone elaborate, because that is the concern to make sure that all of our citizens can find some sort of banking services?

How are you going to reach out to the unbanked? How is it going to help the unbanked?

Mr. MCLAUGHLIN. This something that at MasterCard we have been working on a lot; particularly using prepaid products as an access tool for those who don't have formal banking relationships.

It starts with providing ways to get access to funds themselves so they are not left to the tender mercies of the check cashers and payday lenders. You can look at the work we have done with the Social Security Administration for the electronic distribution of funds and the other ways to allow it to reach these consumers.

We think the key to using mobile will provide people more visibility into their financial information, into their account status so they can be more informed. They can make savvier decisions and we can reach individuals that we haven't traditionally been able to reach through bank branches and other areas.

Mrs. MALONEY. The Federal Reserve has been looking into this, and they did a Federal Reserve report which said that 57 percent of all Americans and consumers surveyed felt that the banking services that they had now were adequate. Then, they looked at people who had mobile banking, and only 12 percent of mobile

phone users reported that they made a mobile payment in the past 12 months; so the technology is out there and people aren't using it.

And given this finding in their report, what actions should be taken by retailers, credit card companies, banks and nonbanks, mobile phone service providers, and others to develop mobile payment opportunities that are tailored to customers so that the customers use it? They say the technology is out there and that people don't even want it at this point, or use it.

Mr. VANDERHOOF. The mobile devices are still just starting to reach the consumers' hands through the mobile networks and through the retail stores that offer them. So we are expecting that there is going to be an increasing number of options available for consumers to be able to upgrade phones with smart card technology that has the ability to support these types of mobile payments. But unfortunately, today, we have a chicken-and-egg situation where we have consumers who want to pay with their mobile device and are waiting for the equipment to arrive for them to use it. When the equipment is available in consumers' hands, then the issuers of these payment instruments that will work on mobile phones will have an opportunity to get them in consumers' hands and merchants will see—

Mrs. MALONEY. That is one barrier. What other barriers exist that could inhibit widespread adoption of mobile payment options? Security concerns?

Mr. LEACH. I would think so. One of the areas that we are addressing is the security of payment card data wherever it progresses.

At the PCI Council, we look technology agnostic at how the data flows into the systems. Many of the terminals that are certified on our Web site have gone through laboratory tests and do have the capability to accept what we are talking about here today. But we are talking mostly on the consumer side. We also have the security of the merchant side and we are seeing rapid growth in the merchant community.

So we talked about unbanked consumers—there have been unbanked merchants. And we are starting to see a new generation of merchants who, before, were not accepting any type of payment other than cash, and now are using such devices as peripherals that you would plug into a smartphone or other types of mobile devices to accept payment. And we are seeing a new industry boom here in the United States.

Mrs. MALONEY. Thank you. My time has expired.

Chairwoman CAPITO. Thank you.

Mr. Renacci, for 5 minutes.

Mr. RENACCI. Thank you, Madam Chairwoman. Again, I want to thank the witnesses for being here today.

Mr. Oliver and Mr. McLaughlin, what effects do you think the current regulatory environment will have on many of these new innovations; and has the uncertain and, really, the changing regulatory environment had an effect on or slowed the evolution of many of these new products?

We will start with Mr. Oliver.

Mr. OLIVER. That is a great question, and one of the important questions that we discussed within this work group; and one of the reasons they asked us to try to rationalize the regulatory infrastructure that might be in place.

Given that most of the payments will be made using existing instruments, I think that people are pretty comfortable with where that is right now and there appears to be no serious legislation on the horizon to change that.

I think the real issue here has to do with those places where gaps occur where different parties are involved in a transaction now than have typically been involved before. The Federal Communication Commission, for instance, oversees the wireless industry, but they have no experience with payments. Many of the payments firms have no experience with that.

And so, that is why this collaborative effort to try to understand whether or not any new regulation at all would be required is a really important first step, we think, on the part of the government, and should occur pretty quickly.

But it is not obvious that there are serious unregulated areas at this time.

Mr. RENACCI. Mr. McLaughlin?

Mr. MCLAUGHLIN. I think it is important to recognize that the mobile phone will be one device, albeit an incredibly compelling device, that consumers will use to access their account.

So from a MasterCard perspective, we want to make sure that all the rights, protections, and privileges consumers have doing that transaction are the same whether they are using a physical card, they are initiating the transaction from a mobile device, or they are shopping online.

And that is the reality for our consumers. They want to be able to trust the transaction and know they are protected, whatever they are using. So we believe in making sure that we aren't creating some separate and independent mobile world, but rather saying these devices are an extension of the rights and privileges that people have today, is essential.

I think it is also important that we allow innovation to flourish in this area. We need to ensure the security and consumer protections. What we can't do is constrain or restrict the ability for industry to determine how to create the most value for consumers and merchants using the new devices.

Mr. RENACCI. Mr. McLaughlin, to move into these type of innovations, there is a scale of investment that has to be made. Can you kind of explain again the scale of investment a company such as yours spends on developing these products and the underlying infrastructure?

Mr. MCLAUGHLIN. Absolutely. And one of the things I think it is important to point out that these are technologies that we have been working on for a decade or more.

We knew that we would want to take advantage of smart devices. We knew that the form factors would be changing. So the first trials we had of contact with technology were in Orlando and Dallas in 2002.

We continue to build and invest. In 2005, as an industry, we began rolling out PayPass, which is the contact technology we have

had. And we worked with all of the participants in the chain, whether it is handset manufacturers, security and chip companies, or telcos, to make sure there is a safe and secure environment to leverage that technology.

So it is an ongoing and substantial investment, not only in the consumer experience in the environment, but in the underlying security infrastructure.

Mr. RENACCI. Thank you.

Mr. Oliver, could you talk about the potential up-front costs that will be required for merchants to accept mobile payments? And is there any danger that they make an expensive transaction, only to have payment technology veer off in a different direction?

Mr. OLIVER. I am probably not the best person to answer a question about what the expense will be for the merchants. But I would like to answer the question about the long-run investments there. Obviously, they are confronted with the issue of trying to understand what the end game is, and therefore make wise choices now.

There are very large merchants who have already made that decision to say, "What do we think will happen in the next 7 years?" And they have said, "We believe mobile technology using NFC contact and contactless cards, as well as current instruments will be there." And they have actually already acquired the terminals to do that.

The incremental costs, from what I understand, of adding that technology to existing terminals is pretty inexpensive. But across a huge footprint for a large retailer, it is going to incur some costs.

But that is what they want to do with this roadmap, to determine what is the end state, and then let us choose how to transition and spend wisely.

Mr. RENACCI. Thank you.

I see I am running out of time, so I yield back.

Chairwoman CAPITO. Thank you. Mrs. McCarthy, for 5 minutes.

Mrs. MCCARTHY OF NEW YORK. Thank you.

And thank you for your testimony. I tend to think that a lot of people would find this really fascinating.

The Europeans have been using this technology for a while. What are the statistics for those countries that are more advanced than us on the breaking in, the stealing of information, their protections?

You already see that information over there. What have you done that is going to be different for here, for us?

Mr. VANDERHOOF. There are several underlying technologies that we have discussed today. The European markets, in particular, have been using this chip technology as part of their payment card infrastructure for many years. And they have proven dramatic reductions in their fraud, because the payment cards now are unable to be counterfeited or the information on that consumer payment product can't be cloned and replicated because of the security of the chip technology.

What is inaccurate is that they have been ahead of the U.S. market in terms of mobile payments. In fact, the U.S. market has a much faster potential for adoption of mobile payments because we have made this investment over the last 5 years in contactless payment card technology.

And therefore, we have hundreds of thousands of terminals already installed in the marketplace that can now use a mobile phone with the same payment capability to make those payment transactions, where in Europe and other parts of the world which have implemented chip technology, they have not implemented chip technology with the ability to interface to a mobile device. So, they are going to require a second investment.

Mrs. MCCARTHY OF NEW YORK. Obviously, we hear a lot about cybersecurity. I know all the nations, NATO; it is their number one issue when they are talking together.

Have you given it any thought, because we are always one step—or hopefully always one step in front of the criminals? This is obviously going to be a big area in the United States, because we have very innovative people who are always trying to—hopefully, you are hiring them, because they always seem to be outsmarting us.

Getting back to the cybersecurity, what mechanisms are out there, when something like that possibly will happen, which many of us agree it will? And how are we going to combat that?

I will throw that out to anybody.

Mr. LEACH. The PCI Council has written standards already to look ahead to where the future is. We are a global standard body, so we already have our standard implemented in Europe with this type of technology.

One of the standards we released last year is called point-to-point encryption. What this allows is for, regardless of the technology, whatever innovation we create here in the United States or abroad, we can encrypt this information, and render it of no value to a criminal.

That way, the system itself can produce and transact, and the consumer can have confidence in that transaction. What we have seen here in the United States, one example is that merchants are taking devices and plugging them into the phone.

And they are now swiping the traditional cards or they are using new mobile technology. They are able to encrypt this information, protect it, before it ever gets into an insecure mobile environment, and are able to process that information securely and safely on behalf of consumers.

So, we do have standards already as an industry. We are looking at new standards, as well as new dynamic ways to make it so that data is of no value. So even if that data is exposed—I share my credit card information with you—we have new technologies that are emerging that would render that of no value to a criminal.

Mrs. MCCARTHY OF NEW YORK. The only reason I am concerned, is we all have our BlackBerries. They are government-issued. But every few days, we get a very long list of those who have actually broken into our BlackBerries, and likely Spam or someone has gotten our information.

So I can understand where the American people might be a little concerned here, because we are supposed to have the protection, yet we are not even supposed to use these when we go overseas. They ask us not to use them.

So, I can see where Americans—you are going to have a big sell for a lot of people, I think. It might take time. And I do know it is used over in Europe quite a bit.

But with that being said, you are going to have to convince an awful lot of people that their checking account is not going to be wiped out.

Mr. MCLAUGHLIN. I think that is what happens any time we introduce new technologies. People are comfortable with the familiar. And that is why our obligation is to make sure every new technology we bring out there is enhancing the security, it is making it safer, so consumers can understand that we can do things using the intelligent devices to make it more secure than what we could ever do with the static, plastic device.

So, that is the advantage of the new technology. But we need to make sure that we are smart about how we harness it.

Mrs. MCCARTHY OF NEW YORK. With that, I yield back the balance of my time.

Chairwoman CAPITO. Thank you.

Mr. Grimm, for 5 minutes.

Mr. GRIMM. Thank you, Madam Chairwoman, for holding this hearing, first of all.

And I appreciate everyone's testimony today.

A couple of questions—Mr. McLaughlin, how much does MasterCard spend annually on fraud? I know that there is quite a bit of fraud now, even traditionally with cards. Do you have a ballpark of how big that problem is for MasterCard?

Mr. MCLAUGHLIN. I don't think we have broken out specific fraud expenses. But what I would say is it is something that we constantly battle. Any change, anything we do, we have to make sure that we are making the system safer for that; so one of the primary focuses of our organization is to make sure that we are eliminating fraud or mitigating it wherever possible.

Mr. GRIMM. Would you say that it increased significantly with the advancements of the Internet?

Mr. MCLAUGHLIN. I think any new technology creates challenges to make sure that it is secure. We have been able to, over the last decade, do a lot to mitigate the fraud potential of what is online. But that is something that we combat every day.

Mr. GRIMM. I will take that as a "yes."

And don't get me wrong, I am all for the new technology. I just recognize that with anything that is new—I slightly disagree with my colleague. I think that criminals are a step ahead of us many times with most of these things, whether it be the Internet, counterfeiting cards originally was a tremendous problem.

Then with the Internet—just now, there was a massive sting operation throughout the entire country, people ordering online and then fencing those items for cash at significant discounts.

The effect on merchants, because I think a lot of the merchants are going to have some issues—when someone comes in and does a transaction, for example if they order over the phone, and they give their credit card over the phone, and then they get their bill and say, "Oh, I didn't order this," the merchant usually eats it. That has been my experience.

Which is really unfair because you have seen—let us just say it is for food at a restaurant. You have delivered to that residence many times, and the delivery boy actually knows the person. But

it might be a college student using dad's card. And this time, dad got the bill and said, well, $45 for this.

They come in and they actually sign for it, then the merchant is protected. So are there going to be safeguards for the merchants, because there obviously aren't going to be any signatures with this. So, that would be a question.

Mr. MCLAUGHLIN. I think you have highlighted one of the most important points of running a payments network or a payments environment. And it is not simply the technologies that are available to us.

Quite often, when we see proposals that are out there or innovations, it is not, "What can the technology do?" but, 'How do you run the network itself, and how do you make sure that you are balanced and fair for all the participants who are in it?"

That is why, as I said earlier, as we adopt mobile technologies, we want to make sure the same protections and rules that we have apply, and the same dispute resolution mechanisms are there.

The goal for adopting the new technologies is to increase the level of verification and certainty we can put around every transaction so issuers benefit from reduced fraud. Merchants also benefit from that reduction in fraud.

Harnessing the new technologies to provide enhanced security and enhanced clarity is the objective. We can do things like providing one-time cryptogram on the individual transaction so we know specifically where it was generated from, moving from static identifiers to dynamic. We can get additional certainty of who you are and the device that you are transacting from, when you do things like an online transaction.

So what we see going forward is the distinction between what is happening at the till, how you purchase online, and other ways that you are transacting; we will move more and more to intelligent devices; and looking to harness the capability of those devices to get us to reduce fraud is the overall goal.

Mr. GRIMM. And then the last question, just on that topic, how about the advanced phishing technology that is out there? When cell phones first came out they were cloning the phones constantly by using phishing technology to steal your I.D. right out of the air. I am assuming that is built into this technology but I think it is worth mentioning since this is an information forum right now.

Mr. MCLAUGHLIN. Absolutely. And that is why—and the reference that Mr. Oliver made to trusted service managers—that is why we want to make sure that anything we do with the new devices is more secure than what we did in the physical card world, so we are more protected against things like phishing and other types of attacks.

Mr. GRIMM. Okay. Thank you.

My time has expired and I yield back.

Mr. RENACCI [presiding]. Thank you.

I yield 5 minutes to the gentleman from Georgia, Mr. Scott.

Mr. SCOTT. Thank you very much, Mr. Chairman.

This is a really fascinating hearing. We are moving so fast with technology that it is hard to keep up with it.

And now, we have a real challenge here, it seems to me, and I have a number of questions, particularly that 91 percent of the

American people now own a mobile phone. That is a phenomenal situation.

First of all, I have questions about who is to regulate this. I am going to start with people who are paying their phones through their mobile units. Who regulates this now? Where does it come under, mobile payments? Is there regulation now?

Ms. MARTINDALE. I think you pose a great question. And everyone kind of goes—there really isn't, when it comes to mobile payments, specifically, the use of a phone to make a non-communication type of transaction; the fingers are pointing in all different directions. And the Federal Communications Commission doesn't appear to, at least, perceive that it has jurisdiction over these types of transactions.

As I pointed out earlier, I think that when a consumer's phone gets stolen, they are going go to the wireless carrier and expect that the wireless carrier has maybe something in the contract, maybe has a policy, and maybe there is a phone agency that is supposed to be in charge. But that is, at best, unclear right now.

Mr. SCOTT. Yes, that concerns me because people lose their phones all the time. The point I am making is if you have 91 percent of the American people, 90 percent of the American people means young people, old people, senior people, people who are getting adjusted to it. So I think that there are some very serious questions here about the regulatory function of it. I also think that there are some issues about the size and the complexity of this issue.

My other major concern is that who really is responsible for monitoring the security risks that are here?

All of these questions really have to be carefully examined. And I think that we have the Consumer Financial Protection Bureau, we have the FCC, we have the FTC. Then we have this little thing in there where, these bills, who pays them? Where do they get the money from? How is it transacted?

In some cases, a telecommunications company pays the bill for them, adds that to their monthly bill and you have, I am sure, within there, all kinds of fee structures, late payments that are piled upon if they don't pay their phone bill, let alone the other bill.

And it just seems to me that the consumer can really get bamboozled here with a lot of financial burden. And yet, right now, this is going on and we don't have a regulator for it.

So my question is where do you all believe this should fall? Is there one agency? Should there be several? Who is going to regulate this?

Who is going do the oversight for this? And particularly, right now, I am sure there are problems in this area. So my concern is this technology is moving so fast we really have to put a priority on how we are going to protect the American consumer, because it is going to move very, very fast. Even right now, with my own cell phone, I have problems just trying to figure out how to get all of this information I am receiving.

And now the other point is too, this is going to have an economic impact someplace. This is going to put a lot of businesses that are in business now out of business. It is certainly going to expedite putting the post office further out of business.

And then there is no paper trail here. If I get my bill, and I am paying my bill, I like to have something in my hand that says, "Hey, I paid this bill. I have a paper trail here."

There is nothing here. It is all in space. So I am just making these points to say we have some work to do.

Thank you, Mr. Chairman.

Mr. RENACCI. Thank you.

I yield 5 minutes to the gentleman from Delaware, Mr. Carney.

Mr. CARNEY. Thank you, Mr. Chairman.

And thank you to the panel for coming today.

I would just like to pick up where my colleague left off and ask the question: What is driving this move to mobile payments?

Why don't we start with Mr. McLaughlin?

Mr. MCLAUGHLIN. Let me open by saying Salesianum, Class of 1983.

Mr. CARNEY. Oh, you would have to do that, wouldn't you—my archrival.

Mr. MCLAUGHLIN. I think it is absolutely driven by the demand we are seeing from consumers. What they are recognizing is that mobile is transforming their lives, particularly younger consumers. They expect to be connected. They expect to have immediate access to information. They expect to have more information and richer information about where they can shop, what deals and offers are available to them and have immediate access.

Mr. CARNEY. So that information would be available on their cell phone, and they would then make some purchase and make the payment through the phone, is that—personally, I don't want my cell phone to do anything more.

I have a hard time keeping track of what it does for me now. And then when I leave it at home, I feel completely lost and naked without my phone.

Mr. MCLAUGHLIN. Yes.

In fact, when you do consumer research they use expressions like "losing a limb," which I found disturbing, when they don't have their phone with them.

I think you are right. I think it has become your GPS. It has become your personal assistant. It has become your alarm clock. It is something that is always on and will progressively be always with you.

Mr. CARNEY. I think several of you have touched on this, but is it more secure?

Mr. MCLAUGHLIN. That is absolutely the objective. We would not move towards this payment environment unless we could enhance the security of what we are doing.

And keep in mind, what we have been able to do with plastic cards in the online authorization network has been a great way to combat fraud. We believe by harnessing mobile devices we can enhance that even further by using the intelligence that is available to it; and then by incorporating consumers deeper into the process of monitoring their finances.

Even without an NFC payment, we can use the phone today. MasterCard has a technology we call "In Control" where I can say, "Let me know on my mobile if an international transaction occurs

or an online payment occurs or a transaction over a certain amount."

So that connectivity gives consumers more information: "How much money is in my account before I make this payment?" It gives them more information—

Mr. CARNEY. That was going to be one of my questions. It would help you not make a payment that you didn't have money to cover.

One of the big things that aggravates folks is when they overdraft their account and get a charge for that. This would help you not do that?

Mr. MCLAUGHLIN. Yes. We can do even better than that. We can tell you exactly, working with mobile banking and other applications, the current status of your account. We can say, "Here is how much you spent against the budget you have set in certain categories," and provide this real-time access to information. So alerts and controls, I think, are essential to the mobile payments experience.

And keep in mind it is the MasterCard network and the underlying account that pulls this together. So in my experience in getting out of—

Mr. CARNEY. Yes, I am breaking in because my time is running out.

How about the unbanked or underbanked?

Let me move on to Ms. Martindale. What is the advantage and how does it work? You mentioned that, I think in your opening statement, for those folks because that is an important group of my constituents.

Ms. MARTINDALE. I think it—the way that you could set it up now so that you wouldn't even need a bank account to do these types of transactions is you could have a prepaid debit card, which is not a bank account.

And you could link your mobile payment application to that prepaid card so that you are drawing down funds from your prepaid deposit. And this is a way that unbanked or underbanked consumers could use these types of—

Mr. CARNEY. You would have to, though, set something up?

Ms. MARTINDALE. Yes, you would have to set something up.

And again, we have a whole host of other concerns about prepaid cards just standing alone because they are as yet not regulated in the same way that a debit card linked to a bank or credit union account already is.

So a prepaid card itself doesn't have any mandatory protections against fraud, theft or errors should your card be lost or stolen or someone rips off your number. And so, if you are adding an extra layer of that mobile payment transaction linking to a prepaid card, we do have a concern that this could—this is a great opportunity to, again, to provide that information in a way that consumers will actually use it.

Unbanked and underbanked consumers are adopting cell phones and smartphones. At the same time, we need to make sure that the payment transaction is covered by some guaranteed legal protections against fraud from the consumer financial protection side, beyond the data security side.

Mr. CARNEY. So, I have 15 seconds left. How do the interchange fees work for this? We had a big debate about that—a dispute about that over the last year. How do the fees work for—would they work for mobile payments?

Mr. MCLAUGHLIN. From MasterCard's perspective, whether you have initiated from a card or initiated from a phone, it is the same transaction.

Mr. CARNEY. Same transaction. Thank you.

I thank the subcommittee.

Mr. RENACCI. Thank you.

I recognize the gentleman from Missouri, Mr. Leutkemeyer, for 5 minutes.

Mr. LUETKEMEYER. Thank you, Mr. Chairman.

I guess, I probably want to start out with, what kind of timeframes do you see all of this developing in? What is the timeframe for general acceptance? What do you see as the timeframe for the problems to pop up and occur here so we know what kind of timeframe we have for some sort of regulatory fix for some of this?

Mr. OLIVER. Can I take the first shot at that?

Mr. LUETKEMEYER. Yes.

Mr. OLIVER. There are a lot of elements of change involved in this and a lot of parties that are going to have to collaborate, release technology, implement technology, educate the consumer, and so forth.

My sense, just as a personal estimate, is that you will see significant deployment in the 2- to 5-year range, because many of the pilots that are currently going on aren't going to be completed until sometime next year. So, I think you are going to see a slow growth curve for an extended period of time.

Mr. LUETKEMEYER. Do the rest of you kind of anticipate the same?

Mr. LEACH. We have been talking about the consumer side of the phone. I think from a mobile payment acceptance, we see that today.

At PIC Council, we have standards that accept certain types of mobile technology to accept traditional payment cards, plastic cards. We have seen our first products come through, be lab tested, certified, and listed on our Web site. So for mobile acceptance, payment acceptance, it is here today.

Mr. VANDERHOOF. Excuse me, I would just add that the solutions on mobile payment that you are hearing from the well-known, well-recognized brands that have a clean sense of the security and the certification requirements of this technology are going to evolve slower than the Internet start-ups of the world who might come up with an application that you can download on your phone and be in business basically overnight.

But for consumers, I think they have to pay attention to who is behind the technology that they might be interested in using? What safeguards exist? And it is probably always the wise choice to look at the established companies that are backing this and the reasons why they are moving at the pace that they are moving in order to maintain security.

Mr. LUETKEMEYER. Yes, I am not very technologically savvy, so this is kind of three steps above my grade here.

But it would seem to me that you are going to have to have a platform here within which all of these transactions can occur with the same sort of technology to be able to talk to each other. I assume that is possible. I am assuming everybody is already working on the same platform or the same language or whatever it takes to make this all work. Is that a safe assumption?

Mr. MCLAUGHLIN. I think you see a strong movement that we work together as an industry to make sure that this will work; that it is safe and secure. So that is why some of the standards that we have talked about earlier like the underlying EMV technology, the PCI standards that are out there, and things of that nature provide a baseline that consumers and merchants know they can trust.

Having those standards out there also allows us to compete vigorously on who can deliver the best consumer experience and the best value out there. So, we have to make sure that there is a foundation that works so we can all compete on the works better.

Mr. LUETKEMEYER. Are there other places in the world where this is being done already? Are we the leading country? Are we technologically leading the world with this application?

Ms. MARTINDALE. Actually we are one of the—we are behind on mobile—

Mr. LUETKEMEYER. We are behind?

Ms. MARTINDALE. Yes, in fact, other countries—people have mentioned Europe—but in developing countries, this is taking off like wildfire, but with a very different set-up, and granted, the infrastructures in those countries may be different. So, I am not necessarily saying that we would be able to replicate in the same way that we have seen in other countries.

I would use Kenya as an example. African countries have been adopting mobile payments using a regular—you don't have to have a smartphone—cell phone, where basically you are giving a deposit to the wireless carrier and the wireless carrier is helping you manage your funds.

And that is something that I have not heard the industry is not as interested in going that direction right now. I think it is more the NFC-enabled, Google Wallet-type of scenario where you have your different payment cards linked up to the application. But other countries have been doing this for several years now, and it has been a way of banking unbanked consumers.

However, it has also involved a great deal of proactive collaboration between the Central Bank of Nigeria, for example, and the major telecoms. It is a very different, more centralized set-up then we would have here.

Mr. MCLAUGHLIN. Yes, I think the key is providing the appropriate technology for consumers. Consumers in the United States today have access to electronic payments. In many of these countries, they don't. So, MasterCard has been working hard to work with the telecommunication providers and financial institutions in those countries to provide appropriate technology.

One quick example—the GSMA is a mobile association, which last year gave us their Mobile Money Innovation of the Year Award for what we had done in Kenya working with Standard Charter Bank and Airtel to provide virtual MasterCard numbers to people who had no access to online transactions on the Internet.

So suddenly, a whole swath of the population who weren't able to access anything online now had access to it by harnessing the existing payment networks and tailoring it precisely for what was needed in those networks.

Mr. LUETKEMEYER. That is interesting. I know the death knell has been sounding for cashing checks for many, many years, and it seems that they are still there. So maybe, you guys are taking a first step down the road to do away with those. Thank you, Mr. Chairman.

Mr. RENACCI. I want to thank all of the members of the panel for testifying this morning.

The Chair notes that some Members may have additional questions for the panel, which they may wish to submit in writing. Without objection, the hearing record will remain open for 30 days for Members to submit written questions to these witnesses and to place their responses in the record.

This hearing is adjourned.

[Whereupon, at 11:18 a.m., the hearing was adjourned.]

A P P E N D I X

March 22, 2012

Prepared testimony of
Troy Leach
Chief Technology Officer
PCI Security Standards Council, LLC

Before the Subcommittee on Financial Institutions and Consumer Credit

"The Future of Money: How Mobile Payments Could Change Financial Services"

Room 2128 Rayburn House Office Building
Thursday, March 22, 2012

Introduction

Chairman Capito, Ranking Member Maloney, members of the Subcommittee, thank you for the opportunity to testify on the important issue of mobile payment security.

My name is Troy Leach and I am the chief technology officer of the PCI (Payment Card Industry) Security Standards Council. The Council is a global industry standards body focused on securing payment card data that is processed, stored, or transmitted regardless of the form factor, device or channel used to initiate payment. Formed in 2006 by the payment card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. to guide the development of open industry standards for global payment security, the Council has an active base of more than 600 global participating organizations representing leading industry players from the around the world.

As the payments environment changes, new technologies are introduced which must be evaluated to determine what new threats may also emerge. It is increasingly important to have a strong framework, driven by cross-industry collaboration to secure payment transactions to contain and reduce fraud for consumers and businesses globally.

Mobile technology offers many opportunities to grow consumer payments and also presents many challenges to secure sensitive payment information. As with any technology being considered for use in a payments environment, the Council's goal is to foster standards that help to minimize this risk to cardholder data. To this end, we have taken a leadership role by actively engaging with industry and other standards groups to proactively address the security of mobile payment acceptance. The Council's work is ongoing, and we have made significant progress.

My testimony today will outline the Council's focus on securing cardholder data, specifically in environments where mobile devices are being used as a new type of payment acceptance tool, and how we're applying our expertise to address the fast-paced evolution and adoption of mobile technology in the payments space. Currently, we are not addressing consumer-facing mobile payment technologies or solutions.

About The PCI Security Standards Council

The Council's Mission

The Council was formed in 2006 by global payment card brands to work with industry stakeholders in guiding the development of open industry standards for global payment security.

Very simply, this means that the Council's goal is to foster standards to protect not just consumers, but also industry players such as merchants (retailers, transportation companies, hotels, etc), banks, government, academia and all other organizations that store, process and transmit cardholder data. It's this wide range of stakeholders that make up the Council's global base of more than 600 leading national, regional and global participating organizations.

The Council's Work

The growth and improvement in payment card security over the past 5 years has everything to do with global industry involvement in the work of the Council.

It's through the voluntary and active participation of this global community that the Council sets and develops technical standards and other resources that comprise the essential tools needed help to protect cardholder data against breaches and reduce payment card fraud. Protecting payment card data is a shared responsibility across the payments ecosystem. Together with our industry participants we drive education and awareness of payment security globally.

Today global adoption of the Council's standards and industry participation in the Council's process for standards development are at an all-time high. As a result of our collective efforts, we are seeing fewer large-scale card data breaches in the marketplace.[1] And when breaches do occur, organizations that have applied the Council's PCI Security Standards are in a better position to mitigate the impact of the compromise.[2] Together these industry standards provide the best baseline available for protecting payment card data. Indeed, other sensitive industries are modeling their own security standards on those developed by the Council.

The Council's Role in Mobile Payments

Our Focus

The Council's focus is the protection of cardholder data through implementation of its standards. Absent such safeguards, that data can be too easily accessed, and then used to commit fraud. It's through this lens that we evaluate mobile payments technology.

---

[1] Verizon Business 2011. "2011 Data Breach Investigations Report."
[2] The Ponemon Institute. 2011. "2011 PCI DSS Compliance Trends Study."

When discussing mobile payment security, it's important to differentiate between two different environments for the use of mobile devices:

1) Merchant acceptance applications where phones, tablets and other mobile devices are used by merchants as point-of-sale terminals in place of traditional hardware terminals, and
2) Consumer facing applications where the phone is used in place of a traditional payment card by a consumer to initiate payment. Several standards groups have been involved and have focused on securing different parts of the mobile payments ecosystem with the aim to protect payment data.

The Council's security efforts to date in this area have been concentrated on work related to securing the use of mobile devices as a point of sale acceptance tool.

In line with the Council's focus on working with stakeholders to secure the entire payment card transaction– from point of entry of payment data to how it's processed through secure payment applications - the Council's efforts in the mobile area are centered around the impact of mobile payment solutions on merchant acceptance and processing channels. Specifically, the Council is focused on mitigating the risk of mobile devices used to take payments from being tampered with; addressing the security of applications running on mobile devices that include or require card data; and the integrity of third-party services. In the midst of an evolving payments landscape and threat environment, maintaining the security of cardholder data remains critical and an ongoing challenge. To address this fast-changing technology and continue to drive payment security forward, the payments industry needs to look to advancements in secure payment technology (e.g., through encryption) to reduce these risks by minimizing the value and exposure of cardholder data, and develop strong effective security practices and controls for mobile payments. The payments industry must take a nimble and proactive approach, while continually evolving our strategies for risk management to adapt quickly to these ongoing changes.

As an open, global cross-industry organization focused on providing baseline standards for stakeholders to increase the security of payment transactions, the Council is well positioned to spearhead this effort. We recognize that payment security is a shared responsibility and requires active involvement from participants across the payment chain. The Council is currently working with stakeholders from all sectors of the emerging mobile payment acceptance environment to collectively and effectively develop the standards and other tools necessary to help secure cardholder data in this manner.

Challenges and Risks

The ability to use mobile technology to accept and process payments undoubtedly offers great potential to the marketplace. However, the rapid innovation and complexity of the environment, present a number of challenges, including managing potential risks to payment information. In the midst of

growing deployment of mobile technologies in payments, worries over security may potentially be a barrier to adoption.

While technologies that promise real solutions for securing mobile acceptance are quickly evolving, a number of security risks remain. These include: rapid and potentially insecure development of mobile applications; lack of traditional security controls such as effective software patch management and monitoring; potentially unauthorized access or too wide-spread privileges of third parties to access financial applications; and to the potential for the abuse protective measures such as data encryption or administrative controls. A failure to adequately address any of these valid concerns can put payment card data at risk.

Our Approach
The Council is applying its expertise to examine these risks within the context of the existing industry security framework that its PCI Security Standards provide – one that's built around the fundamental element of trust essential to enable mobile commerce to flourish.

For mobile technology to be adopted in the same way that traditional forms of payment are accepted, consumers and businesses alike need to be able to trust the ability of the technology to protect their payment data. It's also critical that they trust the service providers and other entities involved.

Trust is even more significant in the mobile payments environment because the environment is fragmented across manufacturers of devices, developers of Operating Systems, application designers, network carriers and the use of various protocols used to connect these different entities. Payment security is a shared responsibility. Ensuring mobile acceptance solutions are deployed securely requires that all parties in the payment chain work together in this effort.

To tackle this issue of trust the Council is working with a variety of stakeholders around the world. The goal is to identify and mitigate the risks that may arise when consumer and merchant roles converge to protect the device, the manufacturing of the device, the secure coding practices for software within those environments and the standards required to test and validate third-party entities that are involved in processing, storing and transmitting transaction data.

Securing Mobile Payments: Payment Acceptance Devices
Mobile phones have not traditionally been built to function as payment acceptance devices. Today, new capabilities are being added to these mobile devices to enable them to accept payment transactions. The integrity of the device that is being used to initiate a payment or access payment card-related information has to be trusted, and this trust must be based on real and robust security. Given this potential risk area to cardholder data, the integrity of the

acceptance device is one of the Council's key focus areas in its work to address the mobile payment acceptance security.

The Council's existing standards include the PCI PIN Transaction Security (PTS) requirements[3] to provide security for physical devices accepting payments, such as point-of-sale terminals at the grocery checkout, gas pumps and airline ticket kiosks. The standard aims to ensure that the device is tamper-proof and if compromised, the data will be "zeroized", rendering it useless. At the end of 2011, the Council expanded the PTS requirements for protecting traditional swipe card terminals against tampering, to apply to mobile payment acceptance devices.[4]

The Council maintains a list on its website of approved devices that have been successfully tested in Council-approved laboratories to assist merchants in assessing the security of their currently deployed terminal devices, and in making informed future purchasing decisions.[5] This list is now expanding to include mobile, as well as traditional, acceptance devices.

Compliance by device vendors with the PCI PTS requirements allows merchants to use plug in devices with mobile phones to swipe cards securely by first encrypting the data at the point that the card is swiped to minimize risk by making it unreadable. The mobile device acts as a conduit and has no ability to decrypt the encrypted data.

Later this year, the Council plans to release specific guidance for merchants on how to effectively use these security requirements in conjunction with encryption technology to more easily and securely accept payments using mobile technology.

Securing Mobile Payments: Payment Software Applications

Today the entire shopping experience, from creating a grocery list to paying for the items on that list, can be realized using mobile technology. Retailers can get more customers through their store during a busy holiday season using payment software applications installed on a phone or tablet that transform these devices into a mobile cash register for quick and easy checkout. Consumers and

---

[3] PIN Transaction Security (PTS) requirements contain a single set of requirements for all personal identification number (PIN) terminals, including POS devices, encrypting PIN pads and unattended payment terminals.
https://www.pcisecuritystandards.org/security_standards/documents.php?association=PTS

[4] PCI Security Standards Council. 2011. "PCI Council Updates PTS Program for PTS, Mobile." Press Release, November. https://www.pcisecuritystandards.org/pdfs/pr_111014_pts_v3-1.pdf

[5] Approved PIN Transaction Security Devices
https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

businesses alike are benefiting from the convenience of mobile payments technology.

The potential for mobile technology to make things faster, easier and cheaper, both at home and in the workplace, domestically and around the world, means there is a growing market demand for businesses to use mobile applications to accept and process payments.

The security of software applications is one of the leading issues in securing mobile acceptance. Applications and acceptance devices must work together to realize a mobile payment transaction. Just as the integrity of the device has to be trusted, so does the integrity of the payment software application. As noted earlier, one of the key roles of the Council is not only to create the standards necessary to enable security, but also to educate the marketplace to the benefit of implementing these standards.

The PCI Payment Application Data Security Standard (PA-DSS) is the Council's standard for addressing the security of software applications.[6] It supports the Council's foundational standard for securing cardholder data, the PCI Data Security Standard (PCI DSS).[7]

Traditional payment applications range from touch screen applications you might see used in a restaurant, to point-of-sale software used in ticketing kiosks in museums and theme parks. Some of these payment applications may be designed to store cardholder data, putting this information at risk. Once again, the Council maintains a list of PA- DSS compliant applications. In this case, that list includes those applications that have been tested by Council-trained security assessors in laboratories and validated as secure. This list is available on the Council website for merchants to use in assessing their own applications and making informed purchasing decisions.[8]

---

[6] To help software vendors and others develop secure payment applications, the Council maintains the Payment Application Data Security Standard (PA-DSS).
https://www.pcisecuritystandards.org/security_standards/documents.php?association=PA-DSS

[7] The PCI Security Standards Council offers robust and comprehensive standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements and support resources to help organizations ensure the safe handling of cardholder information at every step. The keystone is the PCI Data Security Standard (PCI DSS), which provides an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents.
https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0

[8] List of Validated Payment Applications
https://www.pcisecuritystandards.org/approved_companies_providers/vpa_agreement.php

It's against this standard that mobile payment acceptance applications are evaluated, recognizing that the strong technical requirements in this standard should be the baseline for any application accepting or processing payments – whether traditional or mobile.

As part of this evaluation, in 2011 the Council issued guidance on the types of mobile payment acceptance applications that can allow businesses to accept and process payments securely.[9] The Council published a checklist resource to help explain simply and succinctly to anyone currently considering mobile payment acceptance solutions which types of application support PCI Standards.[10] This resource, like all Council tools and resources, is available for download from the Council website free of charge.

The Council also identified the types of applications that fall short of security standards for secure mobile payment transactions. In collaboration with industry subject matters experts, including software application developers, the Council is continuing to examine this area to determine whether the inherent risk of card data exposure in these applications can be addressed by existing PCI requirements, or whether additional guidance or requirements must be developed.

Securing Mobile Payments: The Way Forward

The technology is here to make mobile payments a reality, and the possibilities are infinite. The Council's charter is to provide a forum for collaboration across the payments space to determine how the potential of mobile payment acceptance technology can be realized securely. The more pervasive mobile technology becomes the more we will see new threats and attack vectors that put data at risk. In tandem, other technologies for securing payments will emerge. It is, and for the future will certainly remain, a dynamic space.

As with all unchartered territory, trust must be established to make a way forward. In the case of mobile technology, this means establishing mechanisms and resources to build consumer and marketplace confidence that mobile payments are just as secure as credit or debit card payments. The Council will continue its consideration of extensions to its existing standards and the development of new standards to help ensure the trusted security of mobile payments and the devices that enable them. Additionally, this will mean working to enhance the security of entities across the payment chain who are involved in mobile acceptance, to ensure the existence of an industry standards framework

[9] PCI Security Standards Council. 2011. "PCI Security Standards Council Update on PA-DSS and Mobile Payment Acceptance Applications." Statement, June. https://www.pcisecuritystandards.org/documents/statement_110624_pcissc.pdf

[10] PCI Security Standards Council. 2011. "Which Applications are Eligible for PA-DSS Validation? A Guiding Checklist." Factsheet, June. https://www.pcisecuritystandards.org/documents/which_applications_eligible_for_pa-dss_validation.pdf

to validate these entities, and to establish trust in the services these entities provide. This is an area that the Council will continue to examine moving forward.

In the meantime, great work is being done through the advancement of technologies in payments. The mobile phone will introduce new innovation but also may introduce new risks to payments. Our strategy for minimizing risk that can be added to a payment transaction by a mobile acceptance device is, where possible, to help eliminate card data from potentially insecure mobile environments. Technologies continue to emerge that offer the potential to both leverage the power of mobile computing and effectively reduce security risks by making payment data inaccessible or devaluing the data rendering it useless for committing fraud. The Council has already harnessed some of these technologies to address this dynamic environment and we will continue to assess and develop standards and guidance around them moving forward.

Payment security is a shared responsibility. The Council has engaged a wide range of industry participants in a collaborative effort to apply continued focus to the area of mobile payment acceptance security, including members across the mobile payments spectrum – from those who develop the applications and the phones themselves to those who are providing voice and data services. We are also working appropriately with other standards groups on this issue – such as EMVCo and BITS - and others across the board to address this multi-faceted challenge as an industry. Our outreach efforts to engage new players with whom we can work together to enable security in payments are ongoing.

The mobile payments environment, like other new and complex environments demands an understanding of many different perspectives. As a global industry group with members who represent the payment chain around the world, the Council is positioned to spearhead efforts to help ensure that payment security standards are addressing the mobile payments environment.

Conclusion

Once again, I want to thank Chairman Capito, Ranking Member Maloney, and the members of the Subcommittee for providing me the opportunity to testify on this important issue of mobile payment security. The PCI Security Standards Council's mission is securing payment data, including mobile acceptance. As the payments system changes and new technologies evolve, we will continue to work with our global stakeholders to develop the industry standards and provide the resources necessary for the protection of cardholder data across all payments channels and for the reduction of fraud for consumers and businesses globally.

###

Testimony of Suzanne Martindale
Staff Attorney
Consumers Union of U.S., Inc.
on
The Future of Money: How Mobile Payments Could Change Financial Services
before the
Committee On Financial Services
Subcommittee On Financial Institutions And Consumer Credit
March 22, 2012

Chairman Capito, Ranking Member Maloney and Members of the Committee, thank you for the opportunity to testify about mobile payments on behalf of Consumers Union, the advocacy and policy arm of *Consumer Reports®*.

"Mobile payments" allow consumers to buy products or transfer money with a mobile device. The market includes a range of different technologies, and many ways to fund transactions. The U.S. mobile payments market is still developing, and it remains unclear which trends will prevail. It is too soon to know which consumers will benefit most from the industry's growth – or, inversely, be most vulnerable to risk. However, policymakers can make a few simple fixes to ensure that mobile payments are safe.

The mobile payments market is, in a word, complex. There are multiple ways to initiate payments. Some services involve sending a text message, or using an application downloaded to the device. Others employ a chip embedded in the hardware, which the consumer waves at a contactless reader.

Furthermore, multiple parties are involved in completing a transaction. Consumers, merchants, third-party processors, wireless carriers and financial institutions all play a role in the ecosystem. With so many players involved, the risk of confusion increases should something go wrong. Who is responsible for fixing a problem? If the different parties all point fingers at each other, the consumer may be out of luck.

Despite these challenges, mobile payments in the U.S. are projected to gross $214 billion by 2015,[1] in part due to their potential to provide speed and convenience for

[1] Andrew Johnson, *In Mobile Payments, Lack of Interoperability Threatens Adoption*, AM. BANKER, Dec. 9, 2010, *available at* http://www.americanbanker.com/issues/175_235/lack-of-interoperability-1029690-1.html.

consumers and merchants.[2] Some merchants are also interested in the technology because mobile payment service providers may charge lower processing fees than traditional credit and debit card networks at the point of sale.[3]

Mobile payment technologies also have the potential to serve new audiences. They may appeal to young, tech-savvy consumers, as well as consumers who go outside the traditional banking system for financial services. For "unbanked" or "underbanked" consumers, mobile payments may provide increased access to financial services.[4] Low-income households and households of color in particular are more likely to be unbanked or underbanked.[5] Meanwhile, according to a recent Pew study, cell phone adoption is higher among households of color, as is smartphone adoption.[6] This presents an opportunity for mobile payment technologies to penetrate these markets. However, these same markets may be vulnerable to risk without adequate safeguards.

Internationally, mobile payments have garnered attention for helping consumers in developing countries gain access to financial services. An estimated 5 billion consumers worldwide have mobile phones, while only 1.5 billion have access to financial services.[7] In Kenya, where more consumers have cell phones than have bank accounts, Safaricom's popular M-PESA service enables consumers to manage transactions entirely through their mobile phones.[8] M-PESA customers can deposit or withdraw cash and send money through a network of agents and ATM machines, and can buy goods and services with their mobile phones – all without a bank account.[9]

---

[2] *See, e.g.*, Kate Fitzgerald, Starbucks National Push for Mobile Payments, AM. BANKER, Dec. 6, 2010, *available at* http://www.americanbanker.com/issues/175_232/starbucks-mobile-payments-1029437-1.html. Starbucks' President of U.S. Operations, told *The American Banker* that using mobile payments technology at point of sale was part of their effort to move customers through checkout more quickly. *Id.*

[3] For example, Bling, a mobile payments service that uses contactless readers at the point of sale, charges a 1.5% transaction fee, about half the amount of the usual credit card fee on the merchant. Jefferson Graham, *Customers Pay By Smartphones, Not Credit Cards*, USA TODAY, Dec. 1, 2010, *available at* http://www.usatoday.com/tech/news/2010-12-01-mobilepayments01_ST_N.htm.

[4] The Federal Deposit Insurance Corporation (FDIC) reported in December 2009 that 25.6% of U.S. households, about 30 million, rely on non-banks for some or all of their financial services needs. FED. DEPOSIT INS. CORP., FDIC NATIONAL SURVEY OF UNBANKED AND UNDERBANKED HOUSEHOLDS 11 (2009), *available at* http://www.fdic.gov/householdsurvey/Full_Report.pdf.

[5] *Id.* at 10-11.

[6] PEW INTERNET & AMERICAN LIFE PROJECT, 35% OF AMERICAN ADULTS OWN A SMARTPHONE 9 (2011), *available at* http://www.pewinternet.org/~/media//Files/Reports/2011/PIP_Smartphones.pdf.

[7] Andrea McKenna, *Worlds of Difference in 'Mobile Money' Strategy*, AM. BANKER, Nov. 19, 2010, *available at* http://www.americanbanker.com/issues/175_223/mobile-money-strategy-from-haiti-1028902-1.html.

[8] Safaricom Ltd., M-PESA, http://www.safaricom.co.ke/index.php?id=250.

[9] *Id.* ("M-PESA Services").

However, U.S. consumers have been slow to adopt mobile payments, for several reasons. Some mobile payment systems remain limited in scope and availability. For example, the new Google Wallet uses an NFC (or near field communication) chip embedded in the mobile device, which the consumer waves at a contactless reader to make a payment. However, Google Wallet is only available to Sprint customers with a Nexus S smartphone.[10] Another mobile payments system, Bling Nation, uses a sticker with an embedded chip that the consumer affixes to the device and waves at a reader. However, Bling Nation is still available only through pilot programs in Palo Alto, Chicago and Austin.[11]

Furthermore, market research indicates that consumers have concerns about security of their financial information. In a survey released last week, the Federal Reserve found that over 40% of consumers cited security concerns as a reason for not using mobile payments.[12]

Finally, not all ways to pay with a mobile device are created equal when it comes to consumer protections. Although consumers may not be aware of it, U.S. payments law is fragmented. The level of protections against unauthorized transactions and errors varies depending on whether a consumer links payment to a credit card, debit card or bank account, prepaid card, prepaid phone deposit, or phone bill.[13] Traditional credit and debit cards have mandatory protections under existing law; however, prepaid cards do not.[14] Mobile payments linked to a prepaid phone deposit or phone bill are especially problematic, because they do not fit neatly into existing legal categories.[15] Wireless

---

[10] Google Wallet FAQ, http://www.google.com/wallet/faq.html#payments (last visited June 7, 2011).
[11] Elizabeth Woyke, *Bling Nation Prepares National Rollout of Mobile Payments, Handset Partnerships*, FORBES, Nov. 20, 2010, *available at* http://blogs.forbes.com/elizabethwoyke/2010/11/15/bling-nation-prepares-national-rollout-of-mobile-payments-handset-partnerships/; Dusan Belic, *Bling Nation Expands FanConnect to Austin*, INTOMOBILE, Mar. 29, 2011, *available at* http://www.intomobile.com/2011/03/29/bling-nation-expands-fanconnect-austin/.
[12] BD. OF GOVERNORS OF THE FED. RESERVE SYS., CONSUMERS AND MOBILE FINANCIAL SERVICES 1 (2012), *available at* http://www.federalreserve.gov/econresdata/mobile-device-report-201203.pdf.
[13] *See* Gail Hillebrand, *Before the Grand Rethinking: Five Things to do Today with Payments Law and Ten Prunciples to Guide New Payments and New Payments Law*, 83 CHI.-KENT L. REV. 769, 772-73 (2008) (discussing variation in protections among different payments methods).
[14] Prepaid card funds are typically held in pooled accounts. Regulation E's official staff interpretations appear to exempt funds in pooled accounts from the definition of "accounts" covered by the regulation. *See* Official Staff Interpretation of 12 C.F.R. § 205.2(b)(3), 12 C.F.R. § 205, Supplement I (2011).
[15] At present, these charges are typically for small-dollar text donations or digital content, but some companies are exploring the possibility of paying for other goods and services with prepaid phone deposits and phone bills. *See* Andrew Johnson, *Plan to Make the iPhone a Payment Tool May Accelerate*, AM. BANKER, Nov. 4, 2010, *available at* http://www.americanbanker.com/issues/175_212/iphone-payment-tool-plan-1028195-1.html (quoting Paul Grill, First Annapolis Consulting, who commented on "potential

carriers may provide voluntary protections, but they are typically not disclosed in customer contracts.[16]

The different ways to pay by mobile device, and the varying consumer protections that apply to each, create the potential for confusion when a consumer is faced with a transaction gone wrong. Consumers need to know where to complain and how to get their money back in case of errors or unauthorized use. Consumers cannot afford to lose precious funds due to inadequate protections. For low- and moderate-income consumers, this loss could be especially acute.

Until U.S. payments law is updated to provide clear, guaranteed protections for all payment methods, consumers may be at risk when using mobile payments technology. Nonetheless, a few simple fixes could close gaps in protections and provide clarity to the industry. The Consumer Financial Protection Bureau (CFPB) is in a unique position to address mobile payments, because it has jurisdiction over payment service providers[17] and can clarify regulations implementing federal consumer financial laws.[18] Congress and other federal agencies also have an important role to play in establishing sensible rules of the road that protect consumers and foster innovation. Further dialogue between industry, regulators and consumers is the first step toward shaping a safe and thriving mobile payments market.

Thank you again for the opportunity to testify. I am happy to answer any of your questions.

---

convergence between the mobile and the e-commerce space," in which more types of goods are billed to wireless plan).

[16] Consumers Union reviewed the customer contracts of the top wireless carriers, and found that the protections carriers provide fall short of what consumers get when they use credit cards and debit cards. In addition, many of the protections that wireless carrier representatives maintain that they provide are not disclosed in customer contracts, making it difficult to know whether consumers can count on these safeguards when problems arise. *See* Consumers Union, How Top Wireless Companies Compare on Consumers Protections for Mobile Payments (2011), *available at* http://defendyourdollars.org/document/how_top_wireless_carriers_compare_on_consumer_protections_for_mobile_payments.

[17] Section 1002 of the Dodd-Frank Wall Street Reform and Consumer Protection Act gives the CFPB jurisdiction over "covered persons" providing consumer financial products or services, including payments services. *See* Pub L. No. 111-203, 124 Stat. 1376, 1957-58 (2010).

[18] Title X of the Dodd-Frank Act transfers to the CFPB the authority to write rules under consumer financial laws, including EFTA and TILA. *See* §§ 1002(12) and (14) and 1022(a), 124 Stat. at 1957, 1980.

HEARING ENTITLED "THE FUTURE OF MONEY: HOW MOBILE PAYMENTS COULD CHANGE FINANCIAL SERVICES"

TESTIMONY OF ED MCLAUGHLIN
CHIEF EMERGING PAYMENTS OFFICER
MASTERCARD WORLDWIDE

BEFORE THE COMMITTEE ON FINANCIAL SERVICES
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT
U.S. HOUSE OF REPRESENTATIVES

MARCH 22, 2012

Good morning, Chairman Capito, Ranking Member Maloney, and Members of the Subcommittee. My name is Ed McLaughlin, and I am Chief Emerging Payments Officer at MasterCard Worldwide ("MasterCard") in Purchase, New York. It is my pleasure to appear before you today to discuss developments in mobile payments. The subject of this hearing is a fascinating one, and is on the cutting edge of what is driving change in the way consumers and businesses interact to complete transactions. MasterCard is at the forefront of innovation in this space and a thought leader in mobile payments. We greatly appreciate the opportunity to be here today to share our perspective on how mobile payments are developing and benefitting consumers and businesses.

MasterCard is a Global Payments and Technology Company

MasterCard is a global payments and technology company that connects billions of consumers, thousands of financial institutions, and millions of merchants, governments and businesses worldwide, enabling them to use electronic forms of payment instead of cash and checks. MasterCard has been a leader in the transformation of mobile phones into secure mobile payment devices. We are pioneering the development of unique mobile information services to facilitate and promote financial inclusion and commerce, and we continue to be a champion of

global mobile payment standards. MasterCard also operates the industry's only fully integrated global payment processing platform, which sets the standard for reliability, agility, flexibility, and security. Our platform and technology are fueling a global migration away from cash by enabling safer, less expensive, and more convenient ways for consumers to pay and for merchants to get paid. And, we are proud to be leading this migration by utilizing our assets and resources based right here in the U.S.

MasterCard's technology center, based in O'Fallon, Missouri, drives the software systems and operational network that enables us to seamlessly process billions of transactions representing trillions of dollars each year. Our electronic payment network has the capacity to handle more than 160 million transactions per hour with an average network response time of 130 milliseconds. This is more than twice as fast as our largest competitor. In 2011 alone, MasterCard processed 27.3 billion electronic payments totaling approximately $3.2 trillion, and nearly all of these transactions were processed in our U.S. facility. Through the efforts of MasterCard and other domestic companies, the U.S. is leading a new era of global commerce that will drive value to all participants, deliver greater personal financial empowerment, and offer additional possibilities for paying for goods and services and transferring money to the more than seven billion inhabitants of the globe.

It is an exciting time to be in the payments business, and at MasterCard we are working hard to drive innovations that deliver value to consumers, merchants, and our financial institution customers.

A World Driven By Devices

Perhaps the best way to begin a conversation about what is going on in mobile payments is to acknowledge that there are transformations in consumer behaviors that are happening globally, and these transformations are driven in large part by near ubiquitous access to the Internet, social connectivity, and mobility. We have all seen this in our everyday life, and these trends in technology will continue to rapidly transform commerce. Given the popularity of the mobile phone (more than 4 billion subscribers worldwide), the personal nature of the device (most are carried at all times), and the capabilities of the device (data access, storage, and transfer), it is no wonder that mobile phones are rapidly becoming a popular channel for accessing financial services in-store and online. Mobile phones—and especially smart phones—are giving consumers who already use payment cards a better payment experience.

By some estimates there will be twice the number of connected devices as people globally by 2015. These devices are bringing changes to the way people interact and also to how they want to transact. For example, the acceptance of card-based payments through the use of a handheld device is opening up channels of transactions for entrepreneurs that were not possible a few years ago.

Regardless of the payment environment or device, we need to constantly focus on two goals—making paying for something as simple and compelling as possible for every participant in the payments chain while providing the highest levels of security to consumers, merchants, and our financial institution customers. Intelligent devices such as smart phones provide the opportunity to move both objectives in a positive direction simultaneously, and we invest heavily in technologies that make this duality possible.

As you might expect, smart phones are now providing a platform for the delivery of new applications that are transforming the in-store shopping experience. In a recent survey, over 50% of smart phone users have already used their phone to assist them in shopping in some way. In developed markets like the U.S., smart phones will soon represent over half of the mobile phones in the market. Smart phones provide consumers with the convenience of messaging, browsing, and applications that facilitate commerce. For merchants, smart phones provide a convenient channel to engage consumers at multiple levels, such as though an Internet store-front or a Facebook account, so that merchants can be available to consumers in all of the places where consumers want to find them.

Smart phones themselves are also becoming payment devices through the adoption of Near Field Communication, or NFC, technology. Indeed, major handset manufacturers, including Samsung, HTC, Nokia, and RIM are beginning to deliver NFC-enabled handsets to market, and by 2016 the majority of smart phones will support NFC. MasterCard's *PayPass* technology, which is discussed below, is central to the use of smart phones as payment devices.

Why are these new uses for mobile phones so important? Because they provide convenience and promote financial inclusion in a secure environment. Unlike the simple plastic card that has been around for decades, smart phones provide an intelligent device right in the consumer's hands that the consumer can use to interact with financial services providers and merchants in ways that were never before possible. For example, not only can smart phones provide faster and more convenient ways for consumers to pay, but they can also now enable consumers to access their account information before making a purchase to determine if the transaction is something the consumer can afford. This type of on-the-go budget tool will make more consumers comfortable using mainstream financial products. Smart phones also enable

micro-entrepreneurs to accept payment card transactions, bringing more people into the payment system and empowering small businesses. For example, Square reported late last year that over 750,000 merchants are now using its smart phone technology to accept electronic payments. Companies like Intuit and iZettle also compete in this space for payment card acceptance.

Financial Inclusion

When you look at the 85% of transactions that are still being funded through cash and check, emerging technologies such as smart phones provide an unprecedented opportunity to accelerate the transition to electronic payments and to enhance the lives of consumers, merchants, and communities around the world.

In this regard, we are particularly excited about the global movement towards mobile money. Mobile money creates a unique engine for financial inclusion. By enhancing the reach of our network and services to benefit consumers, we are now able to reach a large number of consumers who are outside the financial mainstream. For example, in markets in Latin America, Africa, and Asia, mobile network operators and financial institutions are increasingly providing access to financial services to the underserved through mobile devices, and MasterCard is working with our partners in these markets to use the assets of our network to help facilitate payments and replace cash. This is particularly so in those markets where the penetration of point of sale terminals that can read plastic cards may be very low.

One example of such collaboration can be seen in MasterCard's recent work with Airtel Africa and Standard Chartered Bank on the Airtel Card. The Airtel Card enables unbanked, underbanked and fully banked Airtel Money mobile wallet customers to conduct on-line shopping on any Internet site that accepts MasterCard in a secure and convenient way through

use of single-use virtual debit cards. The Airtel Card received the award for Best Mobile Money Product or Solution at the 2011 GSMA Mobile Money Congress, where the judges commented that the Airtel Card "provides a developed-world service to the developing world with great use of existing and readily accessible technologies (such as MasterCard's network) to open up commerce and banking to the unbanked and underbanked."

We also believe that payment card solutions like prepaid cards coupled with mobile technology can unlock the global commerce grid to consumers who currently do not have access to financial services. The platforms we have created enable consumers without a traditional bank account to deposit money with a regulated entity or its agent to send money to family members in a distant town or to pay a bill across town, a feat that may have required consumers in the past to travel many miles or to take time off from work. In short, consumers now have new opportunities to access online commerce, transfer funds, pay bills and more. Continuing to invest in our networks will ensure that transactions such as these are made in record time and deliver the most efficient benefits to consumers and businesses alike.

MasterCard's Role In Mobile Payments

As established commerce continues to migrate to new experiences, and newer markets such as digital media goods expand, we are moving not only to a world beyond cash, we are also starting to enable a world beyond plastic. This creates an incredible opportunity for MasterCard and others in the payments business to serve consumers with new experiences and to create value for merchants and other partners who deliver technology-based services to consumers, such as Google and Intel.

At MasterCard, we have invested substantial financial resources and human capital in developing the technology necessary for the mobile payments ecosystem. These efforts have focused on three areas. The first of these is what I will call a contactless-based system. MasterCard's *PayPass* "tap-and-go" product is at the forefront of this space. The second area of the mobile payments ecosystem we are seeing develop is based around SMS-based money management systems, which involve text messaging between mobile devices. MasterCard's MoneySend product is an example of this type of system. Third, as I have already mentioned, we are seeing exciting developments in mobile commerce-enabled systems with the rapid deployment of smart phones, including the innovative MasterCard *inControl* platform.

MasterCard *PayPass*. MasterCard's *PayPass* technology is a contactless payment method that enables consumers to pay with a payment product but without swiping a card. MasterCard has been building the *PayPass* infrastructure over the last decade, focusing on interoperability standards, acceptance locations, security and developing devices. *PayPass* is designed to displace cash for everyday purchases, and enhance credit, debit and prepaid payment products. A tiny microchip and radio antenna embedded in a *PayPass*-enabled card, key fob, device or phone transmit a customer's payment details wirelessly to a high-speed *PayPass* reader at checkout. The reader then verifies the transaction with the customer's bank through the MasterCard network and indicates approval almost instantly.

Encryption technology and MasterCard's Zero Liability protection on a *PayPass*-enabled credit, debit or prepaid MasterCard card make using *PayPass* at checkout as safe as swiping. *PayPass* also has built-in safeguards to help prevent unwanted purchases—it never leaves a customer's hands at checkout, it must be very close to the card reader for it to work, and it only bills the customer once, even if it is tapped twice. As we continue to develop the *PayPass*

program, MasterCard is committed to expanding merchant acceptance in key categories, developing contactless payments for transit, working to expand functionality to mobile phones and other options, expanding beyond low-value payment channels, and increasing marketplace awareness and education. By linking a mobile phone to MasterCard *PayPass*, we bring a new level of convenience to consumers by enabling them to tap and go at any of our contactless-enabled merchants around the globe with the reliability and protections of all MasterCard transactions.

Mobile MoneySend. MoneySend is MasterCard's fully-integrated, on-demand person-to-person mobile payment platform for financial institutions that issue MasterCard products in the United States. Mobile MoneySend is a breakthrough payment platform that provides a better way for consumers to send and receive funds via SMS-text, mobile browser, mobile applet or an Internet PC. Once consumers are registered for MoneySend with their bank, the consumers have the flexibility of directly, easily and securely transferring funds to and from one another through their mobile phone, eliminating the need to write or cash checks, visit ATMs, or wire money domestically.

Senders initiate transfers to any domestic mobile phone number via SMS message, mobile web browser or a downloadable MoneySend application. Upon initiation of the transfer, the sender approves the request by entering the MoneySend mobile PIN which only the accountholder knows. The recipient receives a text message confirmation of the transfer (for pre-registered users) or that the transfer is pending (for yet to be registered users). The funds can then be accessed by the recipient through an account designated during the registration process. These funds are then available for access through the mobile phone. If the consumer has a

MasterCard card associated with the account, the funds can also be accessed at traditional points of interaction, including ATMs, over-the-counter at a bank branch, or at the point-of-sale.

MasterCard *inControl*. MasterCard *inControl* is an innovative platform that offers an array of advanced authorization, transaction routing and alert controls to satisfy consumer demand for increased security and budgeting capability. With *inControl*, spending limits and controls can be set on payment accounts to enable account owners to determine exactly where, when and how their cards are used. Coupled with these controls, real-time email or text alerts can be sent to account owners to provide transparency into the spending activity occurring on the account. For consumers, *inControl* provides a new level of financial control and awareness that is unmatched in today's market. Cardholders create personalized spending profiles for themselves and their family members by setting up spending limits according to budget goals and account security concerns. Cardholders can also choose to receive real-time alerts on specific transactions as well as when spending is nearing a budgeted amount. Because of our substantial investment in innovations like *inControl*, consumers can harness their mobile phones in ways that enables them to manage their finances more efficiently and spend with greater confidence.

Protecting Consumers and Delivering Value

As I mentioned at the outset, we are driven to make payments simple for all participants in the payments value chain, while providing the highest levels of security. This is why we apply MasterCard's Zero Liability protections to new payment technologies, including mobile phone-based payments. The MasterCard Zero Liability policy offers MasterCard cardholders

peace of mind, as in most instances they are not liable in the event of the unauthorized use of a MasterCard-branded product.

Another way we deliver value to participants in the MasterCard network is to ensure that transactions are processed seamlessly and to take steps to combat payment card fraud before it occurs. These are top priorities for MasterCard. We have consistently maintained availability of our global processing systems more than 99.9% of the time. We are able to do this because our network provides multiple levels of back-up protection and related continuity procedures. Moreover, our network features multiple layers of protection against hacking or other cybersecurity attacks, which we supplement with mitigation efforts to strengthen our protection against such threats, both in terms of operability of the network and protection of the information transmitted through the network.

As data is increasingly stored in electronic formats, preventing fraud is more important than ever. Recognizing the importance to cardholders, financial institutions, and merchants of the security of payment card information, and the consumer and other harms that flow from the fraudulent and unauthorized use of such information, MasterCard helped lead the industry in developing the Payment Card Industry Data Security Standard ("PCI DSS"). The PCI DSS is managed by an open governance body, the PCI Security Standards Council, of which all the major payment card brands are members.

The PCI DSS includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. The PCI DSS is intended to help organizations proactively protect payment card account data. We operate several compliance programs in connection with the PCI DSS and otherwise to help ensure that

the integrity of our payment system is maintained by our customers and their agents. Key compliance programs include merchant audits (for high fraud, excessive chargebacks and processing of illegal transactions) and security compliance (including our MasterCard Site Data Protection Service®, which assists customers and merchants in protecting commercial sites from hacker intrusions and subsequent account data compromises) by requiring proper adherence to the PCI DSS. Our customers are also required to report instances of fraud to us in a timely manner so we can monitor trends and initiate action where appropriate. MasterCard continues to work with the PCI Security Standards Council as it develops standards to protect payment card account data in an increasingly mobile world.

In furtherance of our efforts to attack fraud and ensure the integrity of payment transactions on our network, we have recently announced a program to transition MasterCard-branded payment products in the U.S. to the EMV standard. The EMV standard is a global standard for credit and debit payment cards based on chip technology, the objective of which is to ensure interoperability and acceptance of payment cards on a worldwide basis. The adoption of EMV-compliant payment products in the U.S. will help provide additional layers of protection for consumers at the point of interaction, enabling dynamic authentication across all channels and devices—card, smart phone or otherwise.

Conclusion

MasterCard is extremely proud of the role we play in advancing commerce through new technologies. The rise of the mobile phone, and other smart handheld wireless devices, is transforming the way we conduct our everyday lives, and holds significant promise for

delivering new value to consumers and businesses in the delivery of financial services. As I said at the outset, it is an exciting time to be in the payments business.

I appreciate the opportunity to appear before you today and I will be glad to answer any questions you may have.

Prepared Remarks

House Financial Services Committee Hearing on Mobile Payments

Subcommittee on Financial Institutions and Consumer Credit

"The Future of Money: How Mobile Payments Could Change Financial Services"

Richard R. Oliver

Payments Consultant/Retired Executive Vice President, Federal Reserve Bank of Atlanta

March 22, 2012

In 2010, payments research teams from the Federal Reserve Banks of Atlanta and Boston collaborated to conduct an assessment of the state of and potential for the deployment of mobile *payment* options in the United States. Our interests were to determine the impact of mobile payments on existing and emerging payments businesses and to isolate potential risks to consumers and businesses who might choose to use mobile payment solutions. To conduct such an assessment, we invited most of the major players from all aspects of the emerging mobile payments industry to meet with us on a voluntary basis to discuss the opportunities, barriers, and challenges associated with implementing a successful mobile payments environment in the U.S. Attendees included major card brands, wireless operators, financial institutions, industry trade groups, retailers, software providers, processors, handset manufacturers, and suppliers of mobile security technology. Please note that this effort was not directed at mobile *banking*, which is the use of existing remote access web technology to access on line banking functions. Instead, we were focused on the use of mobile phone devices to institute payment transactions at the retail point-of-sale.

Over the course of seven meetings in 2010/2011, we not only gained great insight into the evolution of mobile payments in this country, but we were able to engage what became known as the industry Mobile Payments Work Group (MPWG) in isolating those key factors that must be met to ensure a successful and safe mobile payments offering in the United States.

These factors were based on global experience in the card world and the evolving mobile environment, as well as general knowledge of successful payments systems. The seven factors for success collectively set forth by this group include:

1. The proposed environment would be best defined by the concept of an "open mobile wallet." In essence, the group felt that success was not likely to evolve from a set of dramatically dissimilar proprietary initiatives. The open wallet would support the use of any number of payment credentials, just like the physical wallet does today.

2. The mobile infrastructure would likely be based on Near Field Communications (NFC) contactless technology resident in a smart phones and merchant terminals. Other technologies might exist in parallel, but NFC appeared to be the likely approach due to experiences overseas, evolving standards, and current technology investments by key players.

3. Ubiquitous platforms for mobile should leverage existing payment system rails (debit card, credit card, prepaid card), including the ACH network for non-card payments, and support new payment types that meet emerging needs. This implies the use of traditional clearing and settlement systems.

4. Some form of dynamic data authentication should be at the heart of a layered mobile payments security and fraud mitigation program. Dynamic data authentication involves such traits as one time passwords that negate or mitigate the issue of counterfeit credentials and identity theft. Such technologies are being used in chip and pin card solutions throughout the world today.

5. Standards would be designed, adopted, and complied with through an industry certification program to ensure both domestic and global interoperability. Standards are the key to interoperabilty, security, efficiency, and accuracy. The concept of creating a certification authority to ensure such an outcome would be attractive.

6. A better understanding of a regulatory oversight model should be proactively developed in concert with bank and non-bank regulators to clarify compliance responsibilities. Aspects of mobile payments may fall into areas of uncertainty as to which regulator has oversight. However, it appeared to the group that much of the mobile payment process will likely be regulated based on the payment instrument selected by the end user at the time of purchase.

7. Trusted Service Managers (TSMs) should oversee the provision of interoperable and shared security elements used in the mobile phone. TSMs are organizations that actually create and distribute the secure elements in the phone.

It should also be noted that the MPWG also discussed the potential need for an independent third party to help coordinate the activities of the diverse participants in the mobile payments world to achieve the above listed outcomes. They believed, however, that it was too early in the evolution to decide who such an entity might be or to fully define their responsibilities. Some members of the work group also cited a desire to create an industry "roadmap" that would clarify the nature and timing of future technology investment requirements to reach the desired end state. Once again, however, the group as a whole felt it was much too early to create such a roadmap. Instead, they noted that the results of many planned experiments and pilots, as well as emerging initiatives in other countries, would better inform a roadmap at a later date.

As the discussions of the group progressed, it was determined that the efforts of the group might best be captured and made public through the publishing of a "white paper." Ultimately, such a document was produced by the two Reserve Banks facilitating the effort (see "Mobile Payments in the United States: Mapping Out The Road Ahead", March 25, 2011, FRB Atlanta and FRB Boston). This document not only goes into significant depth on the aforementioned seven principles, but it also serves to define the concept of mobile payments, assess the state of the industry at the time of publication, describe alternative business and infrastructure models, explore the roles and responsibilities of various parties,

set forth the potential opportunities and barriers to success of mobile payments, and to provide insight into the related issues of plastic card security technologies, i.e. chip-and-pin. This paper was widely distributed throughout the payments industry, presented at many conferences, and discussed in the trade press. In addition, the Reserve Banks sponsored a discussion of the paper with Federal regulators and law enforcement agencies in the first half of 2011.

Over the two plus years that the MPWG has met, most of the participants have engaged in one or more mobile payment pilot programs that will serve to "test" the validity of the success factors discussed above. It is important to note that the mobile payments industry is in a very early stage of development in this country, but the market is working properly to explore a variety of implementation alternatives and underlying technology solutions. For example, several partnerships have been formed, handset manufacturers are preparing to deploy phones with imbedded NFC chips, and retailers are acquiring new terminal technology capable of handling mobile payments.

In closing, in parallel with these important market activities, the MPWG continues to meet and is focusing on activities pertinent to achieving the success factors, such as ensuring that security models are well vetted. In addition, the group has been outspoken in asserting the need for a widespread education effort to inform businesses and the public of the characteristics, controls, and value of mobile payments and efforts are underway to fulfill this need.

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

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

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)

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

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

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 device[9] 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.

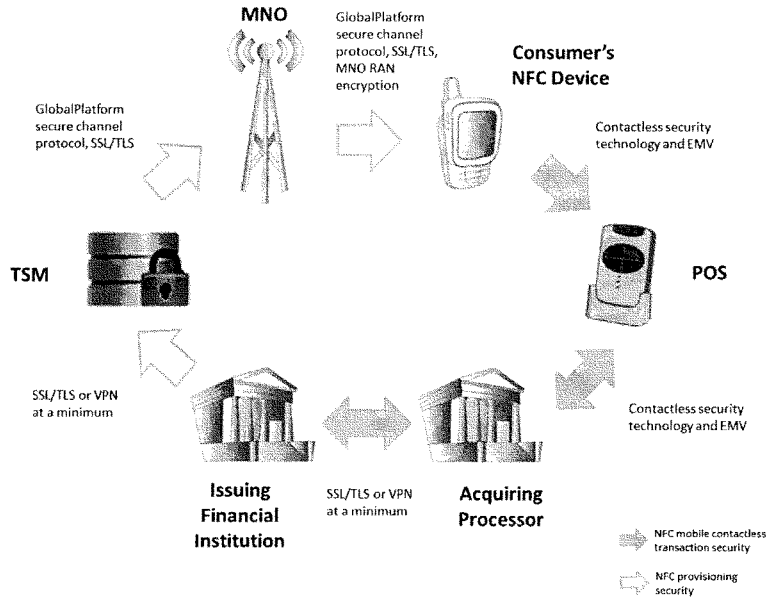
[9] NFC-enabled devices are governed by standards in ISO/IEC (ISO/IEC 18092), ETSI (ETSI TS 102 10 V1.1.1 (2003-03)) and ECMA International (ECMA-340), and by specifications published by the NFC Forum.

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).

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 specifications[10].
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.

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-questionsNFC 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

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.

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.

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.