

**DEVELOPING THE FRAMEWORK FOR SAFE AND  
EFFICIENT MOBILE PAYMENTS**

---

---

**HEARING**  
BEFORE THE  
**COMMITTEE ON**  
**BANKING, HOUSING, AND URBAN AFFAIRS**  
**UNITED STATES SENATE**  
**ONE HUNDRED TWELFTH CONGRESS**  
**SECOND SESSION**  
ON  
EXAMINING THE FRAMEWORK FOR SAFE AND EFFICIENT MOBILE  
PAYMENTS

MARCH 29 AND JULY 10, 2012

---

Printed for the use of the Committee on Banking, Housing, and Urban Affairs



Available at: <http://www.fdsys.gov/>

---

U.S. GOVERNMENT PRINTING OFFICE

77-162 PDF

WASHINGTON : 2013

---

For sale by the Superintendent of Documents, U.S. Government Printing Office  
Internet: [bookstore.gpo.gov](http://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

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

TIM JOHNSON, South Dakota, *Chairman*

JACK REED, Rhode Island	RICHARD C. SHELBY, Alabama
CHARLES E. SCHUMER, New York	MIKE CRAPO, Idaho
ROBERT MENENDEZ, New Jersey	BOB CORKER, Tennessee
DANIEL K. AKAKA, Hawaii	JIM DEMINT, South Carolina
SHERROD BROWN, Ohio	DAVID VITTER, Louisiana
JON TESTER, Montana	MIKE JOHANNIS, Nebraska
HERB KOHL, Wisconsin	PATRICK J. TOOMEY, Pennsylvania
MARK R. WARNER, Virginia	MARK KIRK, Illinois
JEFF MERKLEY, Oregon	JERRY MORAN, Kansas
MICHAEL F. BENNET, Colorado	ROGER F. WICKER, Mississippi
KAY HAGAN, North Carolina	

DWIGHT FETTIG, *Staff Director*

WILLIAM D. DUHNKE, *Republican Staff Director*

CHARLES YI, *Chief Counsel*

LAURA SWANSON, *Policy Director*

CATHERINE GALICIA, *Counsel*

JANA STEENHOLDT, *Legislative Assistant*

BRETT HEWITT, *Legislative Assistant*

MARC LABONTE, *CRS Detailed Economist*

BRIAN FILIPOWICH, *Professional Staff Member*

WILLIAM FIELDS, *Legislative Assistant*

ANDREW OLMEM, *Republican Chief Counsel*

MIKE PIWOWAR, *Republican Chief Economist*

BETH ZORC, *Republican Counsel*

DANA WADE, *Republican Professional Staff Member*

DAWN RATLIFF, *Chief Clerk*

RIKER VERMILYE, *Hearing Clerk*

SHELVIN SIMMONS, *IT Director*

JIM CROWELL, *Editor*

# C O N T E N T S

## THURSDAY, MARCH 29, 2012

	Page
Opening statement of Chairman Johnson .....	1
<b>WITNESSES</b>	
Kenneth C. Montgomery, First Vice President and Chief Operating Officer, Federal Reserve Bank of Boston .....	3
Prepared statement .....	15
Sandra F. Braunstein, Director, Division of Consumer and Community Af- fairs, Board of Governors of the Federal Reserve System .....	5
Prepared statement .....	21
Responses to written questions of: Senator Kirk .....	86
<b>ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD</b>	
“Mobile Payments in the United States: Mapping out the Road Ahead” .....	92

## TUESDAY, JULY 10, 2012

	Page
Opening statement of Chairman Johnson .....	149
<b>WITNESSES</b>	
Michael L. Katz, Sarin Chair in Strategy and Leadership, Professor of Eco- nomics, University of California, Berkeley .....	150
Prepared statement .....	167
Sarah Jane Hughes, University Scholar and Fellow in Commercial Law, Maurer School of Law, University of Indiana .....	152
Prepared statement .....	222
Thomas P. Brown, Adjunct Professor, University of California, Berkeley School of Law .....	154
Prepared statement .....	227



# **DEVELOPING THE FRAMEWORK FOR SAFE AND EFFICIENT MOBILE PAYMENTS—PART I**

**THURSDAY, MARCH 29, 2012**

U.S. SENATE,  
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS,  
*Washington, DC.*

The Committee met at 10:05 a.m., in room SD-538, Dirksen Senate Office Building, Hon. Tim Johnson, Chairman of the Committee, presiding.

## **OPENING STATEMENT OF CHAIRMAN TIM JOHNSON**

Chairman JOHNSON. Good morning. I call this hearing to order, entitled, “Developing the Framework for Safe and Efficient Mobile Payments”. It is an opportunity for the Committee to learn about the growth of mobile payments and the current framework of rules this market operates under.

Our jurisdiction extends over all financial services and payment systems regardless of the company that delivers this service. That is why the Committee needs to make sure there are no gaps in the rules so that this emerging market is safe and efficient. This will be the first in a series of hearings, and future hearings will delve deeper into this discrete policy area.

I would note that today we are exploring mobile payments, not mobile banking. Although both require a cell phone or a smart phone, mobile banking is simply a service that allows consumers to access their bank account over the Internet on a mobile device so that they can perform transactions.

Mobile payments are much more. They allow consumers to pay for a purchase or transfer money using a mobile device. The device takes the place of cash, check, or card. The payment is made through a Web page, a downloadable app, an email, or a text message using a bank or money service business or a mobile network provider.

By simply waving or tapping the device at a terminal, or texting a few letters, a payment is made. At a future hearing, we plan to invite industry witnesses to describe how this works in more detail.

Today’s witnesses are at the forefront of the mobile payments and have spent much time studying this topic. They will describe our country’s current mobile payment system and how it is different from similar systems in other parts of the world. They will also discuss trends in mobile payment use such as who is making mobile payments and how much money is moving through our payment system.

It is not surprising to learn that people between the ages of 18 and 29 are the most active mobile payment users. What may be surprising is that the underbanked make significant use of mobile payments. This can be explained by the high rate of mobile and smart phone ownership across socioeconomic lines.

This morning, we will also explore barriers to use and development of mobile payments in the U.S., opportunities for growth in this marketplace, and regulatory gaps in the various mobile payment models. The current framework of laws that govern mobile payments depends on how the payment is modeled.

If the payment is made through a bank, then the existing set of banking and consumer protection laws apply. If the payment is made through a money service business, then at a minimum, Federal consumer financial, antimoney laundering, and State laws apply.

However, payments made through a text message via a mobile network provider do not fall under banking laws. This Committee began laying the foundation for rules to oversee these new types of payments in the Wall Street Reform Act. The Consumer Financial Protection Bureau was given the authority to apply Federal consumer financial laws to these transactions.

The bottom line is that as the mobile payment system evolves, it is important for this Committee to provide proper oversight so that these payments can be secure and convenient. I look forward to today's testimony, and I now turn to Ranking Member Shelby for his opening statement.

Senator SHELBY. Mr. Chairman, I ask that my written statement be made part of the record so we can move on with the witnesses.

Chairman JOHNSON. Without objection.

Senator SHELBY. Thank you.

Chairman JOHNSON. Thank you, Senator Shelby. Are there any other Members who wish to make a brief opening statement? If not, thank you all. I want to remind my colleagues that the record will be open for the next 7 days for opening statements and any other materials you would like to submit.

Now I will briefly introduce our witnesses. Kenneth Montgomery is the First Vice President and the Chief Operating Officer of the Federal Reserve Bank of Boston. The Boston and Atlanta Reserve Banks have been at the forefront of starting mobile payments. They convened the Mobile Payments Workgroup and produced a white paper that sets out a roadmap for the development of the mobile payments market in the United States.

Sandra F. Braunstein is the Director of the Division of Consumer and Community Affairs at the Federal Reserve Board. Her division authored the Consumer Mobile Financial Services survey we are examining today. I thank all of you again for being here today. I would like to ask the witnesses to please keep your remarks to 5 minutes. Your full written statements will be included in the hearing record.

Mr. Montgomery, please proceed.

**STATEMENT OF KENNETH C. MONTGOMERY, FIRST VICE  
PRESIDENT AND CHIEF OPERATING OFFICER, FEDERAL RE-  
SERVE BANK OF BOSTON**

Mr. MONTGOMERY. Chairman Johnson, Ranking Member Shelby, and Members of the Committee, thank you for inviting me to talk about the Federal Reserve's involvement in the evolution of payment systems in the United States. The Federal Reserve has a keen interest in this topic as part of our broader efforts to foster the efficiency and safety of the Nation's payment systems.

In 2009, the Federal Reserve Bank of Boston began assessing the U.S. mobile payments market to understand mobile payment trends, activities of key stakeholders, and potential risks to consumers related to security and protection.

As part of our assessment and to respond to industry concerns, the Boston and Atlanta Reserve Banks facilitated a meeting in early 2010 with most of the major stakeholders involved in the mobile payments industry. The purpose of this meeting was to discuss the opportunities, barriers, and challenges associated with implementing a successful mobile payments environment in this country, with a focus on mobile purchases at point of sale.

This first meeting prompted the establishment of the Mobile Payments Industry Workgroup, or MPIW, which has met three or four times a year and these meetings are continuing through 2012. Over the course of these meetings, participants have shared their high level plans for mobile payments and their perspectives on the benefits and barriers to implementation.

The workgroup also identified possible areas for future collaboration to build critical mass for mobile payments in the U.S. such as in the area of security and standards. Recognizing that a successful mobile payments platform needed an underpinning on which to build, the MPIW collaborated to define the necessary foundational principles.

The first was to build an open mobile wallet. The concept is a virtual wallet that securely stores multiple payment credentials, as opposed to proprietary or closed wallets that might limit the number of payment methods available for use by a consumer with a mobile phone.

Second, the mobile infrastructure would be based on a standardized near-field communication or contactless technology implemented in mobile phones and retail point of sale terminals allowing users to tap their phones to pay for purchases.

Third, mobile payments will be cleared and settled over existing, well-protected rails, including debit card, credit card, prepaid, and ACH networks. Further, to address security issues during the payment process, dynamic data authentication would be used to deter counterfeiting and ID theft at the point of sale. This is already used in so-called chip and PIN cards in other countries and getting readied for use in the United States over the next 3 years.

Fifth, common standards for mobile payments should be implemented throughout the industry to ensure interoperability, efficiency, and ease of use by consumers and businesses.

Sixth, clarity of regulatory responsibilities among bank and nonbank regulators needs to be established early on. While current regulations and rules may cover underlying payment methods,

multiple regulatory agencies have responsibility for different aspects of payments and wireless transactions. Industry participants urge bank and nonbank regulators, such as the FCC, the FTC, and the Consumer Financial Protection Bureau to collaborate to define the regulatory environment for all participants.

Finally, entities known as Trusted Service Managers should oversee the provision of interoperable and shared secure elements in the mobile phone. These TSMs are the bridge between the banks and the mobile carriers and ensure the process of installing a customer's account information to the mobile phone as efficient and secure.

These principles form the basis of the white paper on the future point of sale mobile payments titled, *Mobile Payments in the United States, Mapping Out the Road Ahead*. The paper, reflecting the general thoughts of the MPIW participants, was written by the Federal Reserve Banks of Boston and Atlanta and published in March 2011.

The paper was socialized at numerous conferences and in the trade press, and shared prior to final publication at a meeting with Federal regulators and law enforcement agencies. The Federal Reserve will continue to facilitate the dialog among the MPIW participants and other stakeholders and monitor progress in the evolution of mobile payments.

A workgroup meeting is scheduled next month. This meeting, which will include bank and nonbank regulatory agencies, will focus on issues related to security, privacy, consumer protection, and respective oversight responsibilities. Future efforts will focus on education that is needed to help consumers understand steps they can take to protect their mobile financial and personal information.

In closing, the Federal Reserve plans to continue to leverage the MPIW as a forum to discuss issues and barriers, collaborate on areas of common interest, and help to ensure that mobile payments evolve safely and efficiently for all consumers. Thank you for inviting me to appear today. I am happy to answer any questions the Committee may have.

Chairman JOHNSON. Thank you, Mr. Montgomery. Ms. Braunstein, you may begin your testimony.

**STATEMENT OF SANDRA F. BRAUNSTEIN, DIRECTOR, DIVISION OF CONSUMER AND COMMUNITY AFFAIRS, BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM**

Ms. BRAUNSTEIN. Thank you. Chairman Johnson, Ranking Member Shelby, and Members of the Committee, thank you for inviting me to appear today to discuss consumers' use of mobile financial services. By mobile financial services, I am talking about two categories of activities.

The first we call mobile banking, which is using your mobile device to interact with your financial institution, doing things you could also do through more traditional means like check your account balance or transfer money between accounts.

The second we call mobile payments, which we define as making purchases, bill payments, charitable donations, or payments to other persons using your mobile device with the payment applied

to your phone bill, charged to your credit card, or withdrawn directly from your bank account.

Beyond banking and payments, mobile devices have the potential to be useful tools in helping consumers track their spending, saving, investing, and borrowing, and in making financial decisions. Such technologies also hold the potential to expand access to mainstream financial services for segments of the population that are currently unbanked or under banked.

That said, the technologies are still evolving and important concerns such as consumers' unease about the security of these technologies must be addressed for consumers to feel confident adopting these new services.

To further our understanding about consumers' use of and opinions about such services, the Board commissioned a survey late last year. Nearly 2,300 respondents completed the survey. This survey integrated questions about using mobile devices for shopping and comparing products, along with questions about using mobile devices for banking and payments. A copy of the report, which is based on the survey responses, is attached to my written testimony.

Nearly nine out of ten adults in the United States have a mobile phone, and two-fifths of those phones are smart phones with Internet connectivity. Among all mobile phone users, one out of five have used their phones to conduct some banking activity in the last 12 months.

Consumers below age 29 have readily adopted mobile banking and make up almost 44 percent of all consumers surveyed who use such services. Adoption rates of mobile banking also differ by racial and ethnic background, with Hispanics and non-Hispanic blacks making up a disproportionate share of those who use mobile banking services.

Of those consumers who had not adopted mobile banking, the primary reason given was that they felt their banking needs were being met through more traditional means. Security concerns were the second-most cited reason for not using mobile banking. Mobile payments are not yet as prevalent as mobile banking. One out of eight respondents reported making a mobile payment in the previous 12 months, and usually this involved paying a bill online via their mobile phone.

Mobile payments are disproportionately used by consumers under the age of 45 and by Hispanics. Consumers who are not currently using mobile payments responded that they were concerned about the security of the technology, did not see any benefit from mobile payments, or found it easier to pay in other ways, for example, with cash or with a credit card.

Consumers who were underbanked, that is, those who have a bank account but also use alternative financial service providers, such as a check casher, a payday lender, an auto-title lender, or payroll card makes significant use of mobile banking and mobile payments. The underbanked are more likely than the general population to use mobile payments, with one out of six using payment services on their mobile devices.

Consumers can also use mobile financial services to make financial decisions. Of those consumers who use mobile banking, more

than two-thirds reported that they checked their account balance or available credit before making a large purchase. Moreover, among the consumers that reported doing this, nearly six out of ten reported that they had decided not to buy an item because of the amount of money available in their account.

Some consumers reported setting up text alerts from their banks if their account balance was getting low, and among those using this service, five out of six reported taking some action in response to receiving these alerts.

We plan to continue monitoring consumers' experiences as the technology and business practices evolve. I am happy to answer any questions you may have.

Chairman JOHNSON. Thank you. Unfortunately, it does not appear that we will reach a quorum for this morning's nominations mark-up. We will, therefore, hold the mark-up off the Senate floor when we vote at 11:30. Please monitor communications from Committee staff for specific details.

Thank you for your testimony. As we begin questions, I will ask the clerk to put 5 minutes on the clock for each Member. Mr. Montgomery, given the evolving marketplace for mobile payments, what are your recommendations for effectively balancing the need for safeguards while fostering efficiency and innovation in this rapidly changing industry?

Mr. MONTGOMERY. We think that there needs to be a balance to ensure that we have an environment where we have cooperation amongst the providers in this complex delivery environment. Mobile payments require a combination of technologies and using our existing infrastructures and payment mechanisms such that there has to be cooperation between the providers, handset manufacturers, and others involved in the payment system.

In that regard, we think that an environment where regulators are working with the structures already in place, will help foster that innovation and where the providers are working collaboratively, setting standards with one another such that the innovation will continue.

The need for standards and interoperability is going to be very important to continue to move progress forward on the adoption of mobile payments.

Chairman JOHNSON. This is for both witnesses, beginning with you, Ms. Braunstein. Information security concerns are one of the biggest barriers to mobile payment use. What steps has industry taken to address those concerns and are they sufficient? What steps should this Committee take to make sure that all forms of mobile payments are secure? Ms. Braunstein, let us start with you?

Ms. BRAUNSTEIN. OK. I think, to be honest, Mr. Montgomery is probably better able to address this question. I know that industry is very concerned about the security, as it is a big consumer issue, and there are things they are doing to address these concerns. Mr. Montgomery could better address those.

Mr. MONTGOMERY. The industry is looking at a number of different mechanisms for security. Security needs to occur both at the channel and in terms of the mobile phone itself. And so, there are standards under development for technologies related to near-field

communication. Likewise, we have to ensure that there is security through the entire channel of delivery, including backing systems.

Sufficient standards exist in place for many of those mechanisms today. Ongoing technology looking at potential security risks across that broad spectrum needs to occur. There is a component of this that involves making sure the consumer is aware of how to use the device and what protections they can take to ensure that their phone is being used for banking appropriately.

Chairman JOHNSON. Ms. Braunstein, what information should a consumer disclosure form contain for a mobile payments service?

Ms. BRAUNSTEIN. So at this point in time, there are no specific disclosures for using mobile technology. The disclosures that apply to the accounts or the mechanisms that people are using to pay their bills would still apply. I think that it bears further study in terms of how effective the current disclosure regime will be over a mobile device.

There are questions of clear and conspicuous. There are questions of size of disclosures for various transactions. And I think that those things have not yet been addressed, but are something that need to be looked at.

Chairman JOHNSON. Mr. Montgomery, the U.S. lags the rest of the world in mobile payment usage. Please discuss why using examples of how this market has evolved in other countries. What were some of the major barriers and how were they overcome? What can we do to encourage the safe growth of this market in the United States?

Mr. MONTGOMERY. So as we look at the market of mobile payments, there are a couple of other countries and implementations that we could look at. In Japan, for example, they have a rather robust implementation of mobile payments. They started with the use of contactless payment cards that were used basically in their transportation system.

In Japan, cash is widely used for payments of lots of services. Over several years, as more and more consumers got accustomed to using contactless technology for transportation, as well as other merchants in particular areas surrounding transportation, they quickly were able to move that technology into secured chips within mobile phones.

As a result, a number of organizations within Japan have collaborated to come up with standards such that mobile handset providers as well as other providers can use similar formats. Restaurants, other consumer outlets now accept that mobile payment device at the point of sale as part of that transaction.

What we see in other countries that do not have as many choices in terms of retail payments, countries like Kenya where they do not have a banking system with lots of branches, is that they are using mobile payments as a way of not only person-to-person payments, but for the ability to get cash and make payments in other outlets. That use relies quite a bit on collaboration between the telecommunication providers as well as the national banking systems.

As we look into Europe, they are likewise moving toward a mobile payment environment, but they have years of experience with the so-called chip and pin card. They are moving to contactless

technology. We see that making consumers comfortable with the use of a contactless card seems to be a segue into getting them comfortable with using a mobile device with the same type of security protections to make purchases.

Chairman JOHNSON. Senator Shelby.

Senator SHELBY. Thank you, Mr. Chairman. Mr. Montgomery, in your testimony, you discuss the need to clarify the regulatory responsibilities among the bank and nonbank regulators for oversight of mobile payments. You note that you believe that the FCC, the FTC, and the Consumer Bureau all have to collaborate to define the regulatory environment for all the participants here.

On which issue is it most important for regulators to cooperate on regulating mobile payments and has the Federal Reserve met with any or all of those agencies to address those issues?

Mr. MONTGOMERY. The regulation for payments using debit cards, credit cards is very well defined. Using a mobile device is just another channel into the payment system. So those rules apply very well.

Senator SHELBY. The rules are there, right?

Mr. MONTGOMERY. Yes, sir, the rules are there. As we look at some other mechanisms by which mobile can be funded, like prepaid cards, as well as perhaps prefunded cards that would be used as part of your mobile payment bill, or perhaps some purchases you would make that would be charged to your mobile payment bill, there are the areas where we seem to need some further collaboration amongst the regulators.

Senator SHELBY. For example? Give us an example.

Mr. MONTGOMERY. So if I was purchasing something and it was charged directly to my mobile phone bill and it cost six or seven dollars, what would be my redress if for some reason I really did not make that charge? Who would I have to go to to get that money back? What would be the regulations so that that telco provider would fund my account? Those are the types of things that we would have to look at.

Senator SHELBY. Is there a lot of that?

Mr. MONTGOMERY. There are some instances in which we are seeing people buying ringtones or other things from their provider and they have to work directly with their provider to purchase those things. Probably another area with similar concerns is the use of prepaid cards, such that if the prepaid card is the funding mechanism, and there was an unauthorized charge, what would be the recourse for getting that card refunded.

Senator SHELBY. Well, today if you have a problem with your credit card, you call your credit card issuer.

Mr. MONTGOMERY. That is correct.

Senator SHELBY. I have had people steal my card, stuff like that. But the issuer always corrects it.

Mr. MONTGOMERY. The issuer corrects that as part of the relationship that they have within banking regulation, and there are rules in terms of the time frames that they have to be resolved, when credits have to be returned. That is not as clear in the mobile world if it was being charged not with your debit or your credit card but with a telco provider or a prepaid card.

And that is the area we think, working with the FCC and the FTC and the Consumer Protection Bureau, we could look at what changes would be required for that.

Senator SHELBY. You want the system to continue to work. I would assume you would not want to be so heavy-handed it would not work, right?

Mr. MONTGOMERY. That is, I think, a very important point, that we are looking for regulation to basically help continue movement in this area, not inhibit the type of progress we want to make. And so, as we look at where there might be gaps in regulation, it would be closing those gaps, not doing a zero-based review with the regulation.

Senator SHELBY. Ms. Braunstein, the underbanked, which are a lot of people, the Fed's recent survey stated that the underbanked are substantially more likely to make bill payments using their mobile phones than the general population. In particular, the report states that 62 percent of the underbanked who use mobile services report paying bills with their mobile phones in the past year, compared with 47 percent of the overall population of mobile phone users.

What are some of the benefits to the underbanked that come from the use of mobile technology? And how do you define the underbanked?

Ms. BRAUNSTEIN. The underbanked—I will take the last question first.

Senator SHELBY. OK.

Ms. BRAUNSTEIN. And the underbanked are defined as people who have a banking relationship. They may have an account at a bank, but they also use alternative financial providers. So in addition to their bank account—

Senator SHELBY. And why do they—excuse me. Why do they do that if they have a banking relationship? Why do they use alternatives?

Ms. BRAUNSTEIN. Well, there could be a variety of reasons why they use—they may need a payday loan or an auto-title loan and it could be the inability to get a loan at a bank. Or the fact that there is discomfort with dealing with banks—

Senator SHELBY. OK.

Ms. BRAUNSTEIN. —and dealing with a payday lender is easier. The accessibility in neighborhoods is also a big reason, where the check cashers and the payday lenders are more accessible to some people who are underbanked, and so they use those services more frequently. It seems that the underbanked are not necessarily underphoned, so they do have a much higher percentage of ownership of mobile phones.

That may be one reason why they are using these mechanisms. There may be a comfort factor with using mobile technology.

Senator SHELBY. The Fed's recent survey also indicated that the use of a mobile phone can have a positive impact on a consumer's financial decisions. For example, the survey found that 59 percent of those consumers who check their bank or credit card account information using a mobile device before making a purchase reported that they decided not to buy an item. They probably saw their balance or thought that they would be challenged.

What are the other ways a mobile device can help consumers make on-the-spot financial decisions?

Ms. BRAUNSTEIN. Well, in addition to the fact that they do not make the purchase, there is also an interesting statistic in terms of consumers who get information about their account balances getting low and take some action such as transferring or depositing more funds to bring the balances up.

The other thing that we are starting to see is consumers using their mobile devices for shopping, and there is the ability for some smart phones, to be used when consumers are in a store to scan in the barcode of an item and get information about similar products, which may be cheaper. It helps consumers make better financial decisions in terms of their purchasing right on the spot.

So it is one of those teachable moments, frankly, in financial education.

Senator SHELBY. It could have a positive impact on consumers' shopping habits—

Ms. BRAUNSTEIN. Correct.

Senator SHELBY. —and make them a little more frugal?

Ms. BRAUNSTEIN. Could be, yes.

Senator SHELBY. Thank you. Mr. Montgomery, in your testimony, you noted that data privacy is a major concern. Providers of the mobile payment services will have access to customer data and a customer's buying behavior, which could in turn be sold to marketers and retailers. We know that.

Your testimony states, and I quote, that the potential marketing value of consumer data, when tied to mobile payments, is significant. I think that is obvious. The question to you, should consumers be given the opportunity to opt out of having their customer information shared in this context?

Mr. MONTGOMERY. Yes. Consumers should have the—

Senator SHELBY. The answer is yes?

Mr. MONTGOMERY. Yes.

Senator SHELBY. OK.

Mr. MONTGOMERY. Consumers need to have the option to opt out from information that is being collected about them. Likewise, as they are using particular services provided by mobile phone and mobile payments, they should be very much informed about what data is being collected.

Senator SHELBY. Thank you, Mr. Chairman.

Chairman JOHNSON. Senator Warner.

Senator WARNER. Thank you, Mr. Chairman. I want to thank you and the Ranking Member for holding this hearing. I know maybe it has not attracted a lot of our colleagues, but I think you are probably looking at one of the most significant areas of growth over the next couple of decades, and I am glad the Fed is taking some of these actions.

I mean, it seems to me you have got two or three different buckets here. You have got, on the mobile payments, you have got the mobile banking piece. You have got the mobile payments piece. You have got the mobile payments piece that runs through the traditional credit card authorization process that comes with a certain amount of protections and rules of the road.

You have got the mobile payment piece that might run, as you mentioned, Mr. Montgomery, back to the telecom provider, right? So the bill might appear there. You have got certain individual retailers who are setting up their own systems where if you come into the national brand retailer, it may then appear back on that particular retailer's credit card or credit device, if they have got some prearranged. And then you have got the prepaid.

Is there any way, at this point, either in the States with your survey you did, or examinations abroad of kind of breaking that into percentages of how much falls into each of those categories?

Mr. MONTGOMERY. I do not have exact percentages, but the vast majority goes back to the credit card.

Senator WARNER. But if you could get some of that and whether the growth is coming in on the prepaid side, as Ms. Braunstein said, in terms of folks who are underbanked, I would be very interested in those, as well as directly back onto the telecom providers' bill.

Because I think one of the things that we might want to think about or love to get you-all's comments on, is that if you are not going to go through the credit card, and we have had more than some debates in this Committee and on the floor about the whole question of interchange fees, and if you affect that fee, whatever level it is set at is the transaction protection fee in there. You could end up having a marketplace set a whole bunch of fees that could be hidden, baked into your telecom bill, or baked into your provider bill, or prebaked into if you have got a prepaid card.

I would just hope we would be—I do not have an answer on what that should look like, but have we been—have you been looking at that? If you are bypassing the traditional credit card industry with the protections that are in place, who is going to bear the risk and who is going to charge the fee to bear that risk?

Mr. MONTGOMERY. Those are some of the issues as we look at, the channels people are using for payment. What are the associated costs that are coming along with that? My earlier comment where I indicated that the vast majority of payments were flowing through the channels that support a debit and credit card, those fees are well-known.

And as we look at some of these other channels, prepaid directly to the telecom provider, that is where we would have to make sure we understood the fee structure.

Senator WARNER. Again, but there are two ways. One may be prepaid, which may or may not carry—you might have a telecom risk. The other would be whether the telecom company is going to take on that risk in terms of bundling into some kind of payment that appears or maybe does not appear on your telecom bill. Is that not correct?

Mr. MONTGOMERY. That is correct. There would be two different areas to look at related to that.

Senator WARNER. And has the work you have done, both looked into how those practices are evolving in the United States and how they have evolved in other countries?

Mr. MONTGOMERY. Not at this point. As we talk about moving forward with some of the work of the Boston and Atlanta Feds and this MPIW and discussions with the regulators, that is where I

would expect we would at least start to discuss some of these issues, and then as other regulators begin to collaborate on them, I would expect some work to occur on that as well.

Senator WARNER. Mr. Chairman, as somebody who felt that we kind of took a blunt instrument to the interchange fee debate, and that echoing Senator Shelby's comments that we want this practice to have appropriate rules of the road but we do not want to inhibit it moving forward, I would urge that we ought to see if we can get some thinking maybe—I know you are going to have other hearings in this area—that kind of get ahead of this, at least in our thinking, because I think this area, you know, somebody's going to bear this risk, different type on prepaid, different type on putting onto the telecom, different type on directly putting it onto the retailers, a specific card, and thinking about that ahead of time so we do not end up later on down the path finding that there is a monster been created here that we did not think about ahead of time and then having to come in and, perhaps with over-regulation later, if we can set the rules before this industry grows too quick.

But I can assure you, as somebody that managed to eke out a living in the wireless business 25 years back when everybody thought it was going to be a tiny little business, and just like this Committee, nobody wanted to show up at the hearing, I would make a bet that this payment system around mobile is going to be a huge issue.

Senator SHELBY. Would the Senator yield, if you would?

Senator WARNER. Of course.

Senator SHELBY. He did more than eke out a living, but he was in the early part of the mobile phone business and everything else. But we want this to grow. I think you would agree. The market will grow it. Innovation will grow it. But we also could choke it to death by regulation and pricing and price fixing, like we did on the interchange fee. Somebody, as you mentioned, somebody is going to pay. There is a cost for all of this, but the more it is, the lower the cost.

Senator WARNER. Right. And all I am saying, Senator—

Senator SHELBY. Would you disagree with that?

Senator WARNER. No, I completely agree and I think you—you know, I agree with you. We do not want to choke this off with over-regulation. But we do need—what we would hate, knowing how quickly some of these industries develop, and there is going to be a clearinghouse at some point because you are going to have all these different systems, trying to at least make sure that we are all aware.

What we would not want to have happen is you have got the beginnings of a robust industry and telecom providers have agreed to bake into a bill X percent, whatever it is, and then after the fact, everybody says, Oh, my gosh, this is way above market, or whatever, and then we kind of back into another interchange argument. We just ought to know what we are getting into ahead of time.

Senator SHELBY. Absolutely.

Ms. BRAUNSTEIN. Senator, can I just—

Senator WARNER. And I know my time is expired.

Ms. BRAUNSTEIN. I am sorry.

Chairman JOHNSON. Ms. Braunstein.

Ms. BRAUNSTEIN. Yes. I am sorry. I just wanted to address one thing in terms of the prepaids, not the telecom bills, but the prepaids. There are some protections already afforded to those prepaids that are payroll cards that are used specifically for paying employees. Those protections have not been extended at this point to general purpose, prepaid cards.

But the authority to do that kind of work has been given to the Consumer Protection Bureau. It was one of the authorities we had under the EFTA Regulation E, that transferred to the Bureau last July. So there is some authority for that right now.

Senator WARNER. The only comment I would make, Mr. Chairman, is, you know, again having been on the telecom side, and I cannot believe that the telecom provider, even with a prepaid, is going to charge the same rate or fee for a text message that my daughter might send to her friend, that they are going to charge for that financial transaction, even with a prepaid chip back to the ultimate receiver of those funds.

Because just the risk exposure is going to be different. Maybe I am wrong. I do not know, but I would like—

Ms. BRAUNSTEIN. Well, at this point, we do not know what will happen in the future, but at this point, from what we can see, the telecoms are not charging for the use of mobile banking or payments. There is no charge.

Senator WARNER. I just would love to have, at some point—and I know we are just at the beginnings of this and maybe we could get some more from the merchants and others and telecoms, and again, a little more idea about what is going on abroad, where this—somebody is going to charge an interchange fee or something like an interchange fee in this process.

I would just like to see what all the options are.

Ms. BRAUNSTEIN. As we said, this is a mechanism to use existing channels. So if you are using a debit card or a credit card, the interchange fees that apply to those instruments—

Senator WARNER. Right, I got that.

Ms. BRAUNSTEIN. —will still apply.

Senator WARNER. I got that. Thank you. Thank you, Mr. Chairman. I appreciate it.

Chairman JOHNSON. Senator Shelby.

Senator SHELBY. I just want to pick up in the area of Senator Warner, just an observation. There is a charge for anything, a service. There should be a charge. People should be aware of this. But I believe myself that the market ought to set it, not the Government, because it is price fixing, in a sense, because as this technology explodes and keeps growing, and it will, as Senator Warner pointed out, price of doing business should come down, not go up.

There is nothing like transparency, but gosh knows, I hope we will not continue down the road of staying in the interchanges. There is just a cost for transactions. I do not mind paying that cost. I know I have got a friend that used PayPal on something. I did not even know how PayPal worked.

But he did it because it was a quick payment like this and he is happy with what he paid. He knew. He is very well-educated. He knew what was happening and he knew it was not free. But as long as people know.

Senator WARNER. And I guess I would completely echo what Senator Shelby just said. I think the market ought to set this, but there are so many ways that you could bake this in that it is not transparent.

Senator SHELBY. Oh, yes.

Senator WARNER. And that is what I was trying to make sure—

Senator SHELBY. I do not like hidden things, but I do not want the Government pricing things. I do not believe the Senator from Virginia does either.

Senator WARNER. No, sir. Thank you, Mr. Chairman.

Chairman JOHNSON. I would like to thank our witnesses for their very interesting testimony today. As the mobile payment system develops in this country and around the world, the Committee must make sure that consumers are protected and that the efficiency and integrity of the U.S. payment system is maintained.

I will look forward to learning more about this topic and working with my colleagues on the policy questions raised by this evolving market. This hearing is adjourned.

[Whereupon, at 10:52 a.m., the hearing was adjourned.]

[Prepared statements, responses to written questions, and additional material supplied for the record follow:]

**PREPARED STATEMENT OF KENNETH C. MONTGOMERY**  
FIRST VICE PRESIDENT AND CHIEF OPERATING OFFICER, FEDERAL RESERVE BANK OF  
BOSTON

MARCH 29, 2012

Chairman Johnson, Ranking Member Shelby, and Members of the Committee, thank you for inviting me to appear before you today to talk about consumers' use of mobile financial services.

My testimony today will discuss development of the mobile payments system in the United States, and activities and progress of a mobile payments industry workgroup (MPIW) first convened by the Federal Reserve Banks of Boston (FRB Boston) and Atlanta in January 2010 to facilitate a discussion among key mobile industry stakeholders as to how a successful retail mobile payments ecosystem could evolve in the U.S. This group includes representatives of several large banks, credit card and automated clearing house (ACH) networks, the two largest mobile carriers, intermediaries/third-party payment processors, Internet payment service providers, mobile technology and security providers, handset and chip manufacturers, mobile and payment trade organizations, and a merchant trade group. Representatives from the Board of Governors of the Federal Reserve and United States Treasury also participate. This workgroup has continued to meet three to four times each year since the initial 2010 meeting.

**Evolution of Mobile Payments and Banking in the United States**

Before turning to mobile payments and banking, it may be helpful to provide brief context about the post- World War II history of the U.S. payments system. Looking back, banks and policy makers in the 1950s and 1960s were grappling with significant problems created by the growth of economic and financial activity relative to our ability to process paper payments and other financial instruments. At that time, retail payments were largely made by cash and checks. The use of computers to automate banking processes was just beginning. Since then, the U.S. payments landscape has changed dramatically. Electronic payments made through payment card networks and the automated clearing house system have become increasingly prevalent, and now represent about four out of every five noncash payments in this country. Virtually all check payments, which have been declining in number since the mid-1990s, are now cleared electronically, rather than in paper form. The cumulative effects of automation and innovation have driven several waves of new banking and payment services that continue to improve the efficiency and effectiveness of our payment systems.

The evolution of mobile banking and payments encompasses a combination of continued advances in hardware, software, and payment systems, including contactless payments, online banking, mobile phones (particularly smartphones), applications, and the convergence of Internet or e-commerce and mobile-commerce.

Since the late 1980s, companies and industries around the globe have experimented with different payment mechanisms aimed at improving access to banking services and the efficiency and ease of use for retail point-of-sale payments. For example, a contactless technology was developed in Japan, which a major commuter railroad in Tokyo implemented in a proprietary reloadable prepaid card. In addition to transit fare, consumers could use the contactless card to pay for purchases at merchants equipped with contactless readers near train stations. A similar product, also based on this contactless technology, was launched in Hong Kong's transit system in 1997. In the same year, a RFID<sup>1</sup> contactless payment system that allowed customers to wave/tap a fob to pay at the pump, was launched, the first of its kind in the United States.

In the late 1990s, Finland launched a number of mobile commerce and banking initiatives. The first two mobile phone-enabled vending machines, which accepted payment via mobile phone text messaging, were installed in Helsinki. A bank in Finland launched the first mobile banking service to monitor account activity using this technology.

In the early 2000s, an online payment platform emerged that allowed consumers to email payments to each other. In 2002, online auctions were enabled to receive electronic payments from participants, replacing paper checks. Eventually, the online payment platform was expanded to online merchants.

U.S. consumers began to embrace online banking in the early 2000s. By October 2002, 34 million consumers, (representing 30 percent of U.S. Internet users) used

<sup>1</sup> RFID or Radio Frequency Identification Device is a tag or transponder used to identify and transmit data short distances in one direction via radio waves.

online banking, an increase of 19 million consumers performing online banking since March 2000.

Initiatives that would allow consumers to use their mobile phones to perform new functions surged in 2000, driven by the development of mobile Internet access, the popularity of the Internet and e-commerce, and the increased awareness of mobile phones as more than voice communication tools. However, these service offerings did not meet consumer expectations and neither the phones nor the mobile networks handled data well, which led to very low adoption rates. The arrival of 3G<sup>2</sup> services in the mid-2000s addressed earlier technology problems and had a revolutionary impact on mobile technology in the U.S. Mobile phone manufacturers introduced smartphones that were enabled with more effective Web browsing and data capabilities.

By 2006, helped by increased Internet and online banking adoption, and availability of smartphones, banks began to reexamine the development of mobile banking capabilities. Six of the largest ten U.S. banks offered mobile banking services by the end of 2007. Initially most banks offered browser and Short Message Service (SMS) based services, but in 2007, the mobile banking/payments market underwent a major transformation with the introduction of a new generation of smartphone. Now customers were able to download banking applications and other more advanced applications used for mobile-commerce that were not SMS-based, providing customization and improved security. The success and rapid growth of these and other smartphones led to increasing use of downloadable mobile applications for mobile banking and payments. By 2008, core deposit processors and mobile solution vendors began to develop software solutions tailored to financial institutions, enabling smaller U.S. banks to also offer mobile banking services.

Beginning in 2005, two payment networks launched several U.S. card and mobile contactless trials, which typically took place in metropolitan areas and ran for 4 to 6 months. The trials involved using a mobile phone to pay for in-store purchases at selected convenience stores and fast food restaurants, purchase transit tickets, or purchase concession items at sports venues. Although some trials proved the viability of Near Field Communication<sup>3</sup> (NFC) contactless technology, no full-scale deployments followed. In 2009–2010, several NFC initiatives were taking place in Turkey, Singapore, and the U.K., and NFC-enabled phones were introduced in Canada.

Several new mobile payment services were introduced within the last 3 years that could have a major impact on mobile payments in this country. In 2009, a new attachable card reader that plugs in to a smartphone was introduced, enabling small merchants to accept credit and debit cards. In 2011, a number of companies and industry partnerships announced mobile/digital wallet solutions utilizing NFC or cloud technology.

Mobile payments have been referred to as the “next payments revolution” by some industry participants. As mobile wallet technology, built upon the NFC contactless chip and secure element<sup>4</sup> for improved security and convenience, appeals to a broader array of consumers, and as merchants, banks, payments systems participants, and technology and telecommunications providers derive increased revenue or lower costs as a result of broad adoption, mobile payments should significantly change domestic and global payments practices.

#### **Why the Federal Reserve System Convened the MPIW**

The Federal Reserve strives to foster the safety and efficiency of the Nation’s payment systems. We monitor the evolution of retail payments through a variety of means, including a triennial Retail Payments Study<sup>5</sup> and an annual Survey of Consumer Payment Choice.<sup>6</sup> Of particular interest has been the migration of retail payments from traditional to emerging platforms, including the evolution of mobile banking and payments.

When FRB Boston began to research mobile banking and payments, our goal was to better understand how the industry was evolving, the factors that would motivate interaction and cooperation between mobile carriers and U.S. banks, the major barriers to adoption, and the impact of mobile payments on consumers in the U.S. payment system. We had seen mobile payments evolving more quickly in other parts

<sup>2</sup> 3G (generation) mobile services provided more bandwidth for faster Internet access from a mobile phone, as well as advanced media features.

<sup>3</sup> Near Field Communication or NFC is a short-range wireless proximity technology that uses radio frequency to enable two-way communication between devices. NFC chips are embedded in mobile phones to enable contactless “tap and go” payments.

<sup>4</sup> Combination of hardware, software, interfaces, and protocols that enable secure storage and use of credentials for payment, authentication, and other services.

<sup>5</sup> [http://www.frbservices.org/communications/payment\\_system\\_research.html](http://www.frbservices.org/communications/payment_system_research.html)

<sup>6</sup> <http://www.bos.frb.org/economic/ppdp/2011/ppdp1101.htm>

of the world and wanted to understand why progress in the U.S. was slower. In late 2009, the large U.S. banks were developing mobile banking solutions, and regional and small banks were beginning to assess their business cases for mobile banking, but the concept of using a mobile phone to make a purchase was just surfacing.<sup>7</sup>

In conversations FRB Boston had with bankers and payments experts in 2009, we heard that they were concerned with fragmentation and lack of communication among key stakeholders, particularly mobile carriers, about the direction of mobile payments in the U.S. Industry participants suggested that the Federal Reserve facilitate a conversation among a diverse group of mobile payment stakeholders. Realizing that mobile payments would impact consumers in new ways, we wanted to ensure that all stakeholders adequately addressed issues related to consumer protection and security. Additionally, mobile carriers, which had limited understanding of banking and payment systems, would have an important role in the evolution of mobile payments, which introduced new coordination issues. Lastly, we believed that mobile payments, correctly implemented, could create new efficiencies in payments and possibly create new, cost effective, alternatives for the unbanked and the underbanked. As a result, the Federal Reserve hosted the first meeting of the MPIW in January 2010, to facilitate discussion on the evolution of mobile retail payments in the United States.

### **Objectives of the MPIW**

The overarching goal of the Federal Reserve in convening the MPIW was to encourage growth and innovation in the mobile payments market while minimizing risk to consumers and the payment system. The Federal Reserve believed it was important to gain an industry perspective to determine what barriers existed to the proper evolution of this market and whether we could help eliminate these barriers. We also wanted to explore how we might collaborate on issues of mutual interest. Thus, the objective for the first meeting was to have the experts inform and educate us, and to engage in an open cross-industry dialogue.

Many of the organizations represented at the meeting were already involved in mobile payment initiatives in Asia, Africa, and Europe. In the U.S., a variety of very limited NFC contactless pilots were underway that enabled contactless payments initially on credit and debit cards and then mobile phones, but none with any lasting commercial availability. The industry was struggling to define a direction for mobile payments because of conflicting business models and strategies, and a lack of demonstrated consumer demand.

The main objectives for the group were to (1) gain a mutual understanding of the evolution of mobile retail payments in the U.S.; (2) provide a forum for participants to assess challenges, find points of mutual value, share ideas, and build consensus in a nonbinding, free market manner; and (3) identify possible opportunities for future collaboration to help build critical mass for the success of mobile payments in the U.S.

### **What the MPIW Has Completed to Date**

Recognizing the diversity of industries in the MPIW, subsequent meetings attempted to level set the group by covering each organization's initiatives relative to mobile payment plans, and perspectives on the benefits and barriers to implementation. Participants identified as benefits of mobile payments:

- The ability to reduce fraud using an encrypted contactless mobile platform.
- Potential merchant cost efficiencies gained by processing mobile payment transactions considered more secure than card transactions because of the use of dynamic data versus static magnetic card data, and reducing potential costs associated with PCI (Payment Card Industry) security standards compliance.

<sup>7</sup> Banks had shown significant interest in the previous 3 years, but many preferred to be fast followers, not leaders. Most banks, except the very large, were moving slowly, waiting for others to demonstrate the viability of mobile payments. Only 1,000 of the approximately 17,000 banks offered mobile banking in the U.S. at the end of 2009. However, 40 percent of U.S. consumers used online banking. Many stakeholders believed that in 2010 and 2011 there would be significant momentum leading the financial services industry to become more involved in mobile (banking and payment) services. They noted, however, that many smaller U.S. banks and credit unions look to their existing third-party core deposit processors to deliver solutions without significant upfront cost.

Contactless cards, introduced several years ago in the U.S., were not successful and did little to generate demand for mobile payments. Poor marketing and education may have contributed. Many cardholders received contactless cards but were unaware that they had them or how to use them and did not know whether merchants they frequented accepted contactless payments.

- Consumer convenience and value using a mobile wallet containing multiple payment methods stored securely in the mobile device, along with loyalty cards, virtual coupons, and discounts customized to reach different demographic cohorts determined by location-based, real-time capabilities of mobile technology.
- The ability to use a mobile phone to provide financial services to the unbanked and underbanked consumer segments.

Despite the benefits, participants identified a number of barriers that have impeded the growth of mobile payments, including:

- Lack of consumer demand, driven by the availability of many safe alternative payment choices in the U.S. and few differentiating factors or substantial benefits that consumers can see yet from mobile payments.
- Lack of NFC-enabled smart phones. This obstacle may be partially addressed as several handset manufacturers have committed to making more NFC-enabled phones in 2012.
- Lack of a standard business model (bank-centric, carrier-centric, partner- or nonbank-centric), creating market fragmentation and limits mass adoption.
- Small percentage of merchant terminals that accept contactless NFC payments today. The capital investment in point-of-sale equipment for contactless technology is expensive, so merchants have been reluctant to make investments until they are certain of the direction in which the market is headed. They must now also factor in the implementation of EMV technology in the U.S., given the recent Visa/MasterCard mandate of compliance beginning in 2013.<sup>8</sup> However, this mandate may encourage faster implementation of NFC as part of the EMV implementation, or at least provide a deadline for compliance.
- Uncertain revenue models and lack of collaboration. Two NFC mobile wallet providers are aggressively seeking merchants to participate in their programs, and offering incentives for eligible consumers to use their mobile phones to pay for purchases. These commercial trials test new revenue models and partnerships to determine whether collaboration among stakeholders is successful.
- Participants also identified other barriers, such as the uncertainty regarding who owns the customer relationship (banks or mobile carriers), lack of global standards, and unclear regulatory direction as hindering the growth of the market.

Building on the identified benefits and challenges, the MPIW discussed the need for a roadmap to develop a high-level framework for the U.S. mobile ecosystem. This roadmap would include best practices and industry standards to manage the technology, security, settlement risk, and customer requirements at different points in the value chain. The MPIW also wanted to understand the roles of regulators for mobile payments and the applicable regulations. The MPIW then worked to define the principles essential to addressing the barriers and ensuring a successful mobile payment ecosystem in the U.S. Participants agreed in general with the principles related to mobile security, interoperability, and consumer protection, although there was not unanimous support on all details. These principles formed the basis of a white paper on the future of point-of-sale mobile payments in the U.S., *Mobile Payments in the United States Mapping out the Road Ahead*, published in March 2011.<sup>9</sup> Although written by the Federal Reserve, it reflected the general thoughts of the MPIW. These foundation principles are summarized below:

- Creation of an “open mobile wallet” that supports multiple payment options (credit, debit, bank account, prepaid/stored value, *etc.*) stored in a secure element in the phone, with broad payment and merchant marketing value options, such as rewards, coupons, and loyalty programs, enabling consumer choice.

<sup>8</sup> EMV is a global standard for credit and debit payment cards based on chip card technology, taking its name from the card schemes Europay, MasterCard, and Visa, which developed it. The standard covers the processing of credit and debit card payments using a card that contains a microprocessor chip at a merchant payment terminal. The transactions are referred to as “chip and PIN” because PIN entry is usually required to verify the customer is the genuine cardholder. The EMV standard has been implemented in most developed countries, other than the U.S. In August 2011, Visa announced a phased EMV migration plan for the U.S. In January 2012, MasterCard announced its own EMV adoption program. Both programs incorporate similar incentives and timelines designed to encourage migration by processors and acquirers by April 2013, and retailers by mid-2015 (2017 for automated fuel dispensers).

<sup>9</sup> <http://www.bos.frb.org/bankinfo/firo/publications/bankingpaypers/2011/mobile-payments-mapping.htm>

- Use of NFC technology for contactless mobile payments at point-of-sale, along with enabling secure mobile applications. NFC must be based on industry standards, capable of supporting all payment methods and networks, and operable globally and in multiple venues (*e.g.*, retail, transportation, ATM).
- Clearing and settling payments through existing channels (credit, debit, prepaid, ACH, mobile), but open to new channels. Existing payment mechanisms are the necessary foundation for the mobile payments platform to allow for mass adoption and consumer choice. New payment channels should be permitted but must be interoperable with the existing clearing/settlement system.
- Deployment of dynamic data authentication (DDA) as part of the security and fraud mitigation program for card-based mobile payment transactions. DDA generates a unique one-time cryptogram for each transaction, which is verified by interaction between the encrypted information on the chip and the network server when the transaction is authorized. Using contactless chip technology for mobile payments can reduce fraud because even if payment card information is stolen it cannot be used to make counterfeit cards or fraudulent online transactions.
- Development of mobile payment standards for the U.S. based on international standards and an industry-supported certification process to ensure domestic and global interoperability. The MPIW discussed potential gaps in standards for rules and best practices, and possible existing banking standards or rules that could be applicable to mobile phones with some modification. The payments business has well-defined groups that set standards, such as the American National Standards Institute and NACHA. Who would promote the adoption of the standards by the mobile payments industry is an open issue. Participants suggested that the U.S. consider working with existing mobile standards bodies, such as GSMA, GlobalPlatform, and NFC Forum, as appropriate, to identify gaps in coverage, and develop globally interoperable standards.
- Clarity of regulatory responsibilities among bank and nonbank regulators needs to be established early on, with input from the mobile stakeholders. While current regulations and rules may cover underlying payment methods, there is confusion because multiple regulatory agencies have responsibility for different aspects of payments and wireless transactions. Industry participants urged bank and nonbank regulators, such as the Federal Communications Commission, the Federal Trade Commission and the Consumer Financial Protection Bureau, to collaborate to define the regulatory environment for all the participants. For example, data privacy was a major concern. Complexities arise when different parties begin to share data. The potential marketing value of customer data when tied to mobile payments is significant. Data must be managed carefully to avoid potential abuse and unauthorized access to mobile payments data (*e.g.*, transaction data, location-based data, *etc.*).
- Trusted Service Managers (TSMs) should manage and control the provision of secure elements in the mobile phone to control risk and ensure interoperability between mobile platforms. Although a broader role for the TSM was mentioned, the MPIW believed it was too early in the mobile payments evolution to consider this option.

Several major initiatives occurred after the paper was published in March 2011. First, the Federal Reserve and MPIW members began discussing the basic principles at payment industry conferences, and with payment trade groups, individual organizations, and regulators to collect feedback and escalate issues.

Second, to get input from a broader group of stakeholders, we invited several merchants, a prepaid card provider, debit card networks, a global mobile standards body, and consumer-focused organizations to the July 2011 MPIW meeting. The merchants raised several issues. They remain concerned about their business case—processing costs, investment in terminal upgrades, and cost of PCI compliance. Merchants would like to collect marketing data that will enable them to offer loyalty programs, customized coupons, and merchant rewards that provide consumers with a better shopping experience and increase sales. Because of the large capital investment, they would like to see a roadmap that clearly illustrates the industry direction for mobile payments, including mobile wallets.

Third, we created a sub-group to identify security pros and cons related to retail mobile payments that use contactless NFC (SIM, micro SD and embedded chip) or cloud technology. FRB Boston plans to publish a report of the findings later this year.

### **Current Status of the U.S. Mobile Payments Landscape**

The volume of mobile Internet and remote purchases (m-commerce) is still small, but growing as the number of mobile applications increases, and more consumers own smart phones (about 45 percent adoption in the U.S. currently). As consumers have more opportunities to receive mobile coupons, discounts, rewards and location-based offers, the incentives to use mobile payments will further increase.

NFC contactless technology is being implemented in conjunction with several mobile wallet solutions at retail point-of-sale locations; however, alternatives to NFC do exist. QR codes<sup>10</sup> are in use at a few retailers for prepaid mobile purchases. Cloud technology, where payment credentials are stored on a secure file server that communicates with the merchant terminal for payment, rather than in a secure element on the physical mobile phone, is another emerging alternative. In the current mobile market, some of the large players continue to invest in NFC, others are developing wallets in the cloud, and still others are covering all bases by providing mobile services for both NFC and cloud. It is feasible that these technologies will coexist in the mobile payment ecosystem.

Nonbanks are substantially influencing the evolution to mobile payments. In 2011, several commercial partnerships and joint ventures were announced for retail mobile wallet payments. Additionally, an online payment platform announced plans to enable brick-and-mortar merchants to accept payments from its wallet accounts. The initial offering uses a mobile phone number, not a mobile phone. Several new entrants to the payment system are enabling small merchants to accept card payments using their mobile phones with a plug-in device and a mobile application, while others serve as intermediaries to handle payments for digital content billed directly to mobile carriers.

Some smartphones are being used for functions previously performed on personal computers. These devices became a game changer because they provided consumers with an interface to the Web and many new applications. Consumers demonstrated their desire to use their smartphones for multiple functions, which led to even more new applications. The smartphone helped to build consumer experience and prepare the environment for mobile payments.

### **Next Steps**

The Federal Reserve will continue to facilitate the dialogue among MPIW participants and other stakeholders and monitor progress in the evolution of mobile payments. The next MPIW meeting is scheduled for April 2012. This meeting, which will include bank and nonbank regulatory agencies, will focus on issues related to security, privacy, and consumer protection, and respective oversight responsibilities. Future MPIW efforts will focus on education that is needed to help consumers understand steps they can take to protect their mobile financial data, including using passwords to lock their devices to prevent access to sensitive data, mitigation tools that allow for remote device deactivation and wiping of data, and alerts of suspicious activity.

The Federal Reserve will continue to conduct research to better understand consumer needs, behaviors, and adoption plans related to mobile payments. In addition, the Federal Reserve plans to work with industry participants to identify potential gaps in security and fraud prevention, and potential mitigation strategies for the different mobile payment technologies (NFC versions and cloud). We plan to encourage the mobile stakeholders to work together to define the respective responsibilities of the various parties (*e.g.*, the phone, mobile carriers, processors, banks, and settlement systems) to ensure robust end-to-end security, and to develop security rules and standards for eliminating or appropriately mitigating risks for mobile payments.

### **Conclusion**

Collaboration among mobile industry stakeholders, the Federal Reserve, and interested Government agencies through the MPIW has helped to educate diverse participants on different views and concerns around mobile payments, and awareness of the need for collaboration in certain areas, such as security and standards. Going forward, the MPIW will continue to provide a forum to discuss issues and barriers as they arise with an objective of more timely resolution. The MPIW enables proprietary innovation to occur, while promoting a shared framework for interoperability. Finally, working with mobile carriers, banking and payments industry participants, and Government regulators, the Federal Reserve hopes to help mobile payments in

<sup>10</sup>For mobile payments, QR codes are two-dimensional barcodes that can be read by smartphones with a mobile application to pay for purchases or receive mobile coupons.

the United States evolve in an efficient and safe manner and provide a convenient payment option to all consumer segments.

Thank you again for inviting me to appear today. I am happy to answer any of the Committee's questions.

---

**PREPARED STATEMENT OF SANDRA F. BRAUNSTEIN**

DIRECTOR, DIVISION OF CONSUMER AND COMMUNITY AFFAIRS, BOARD OF GOVERNORS  
OF THE FEDERAL RESERVE SYSTEM

MARCH 29, 2012

Chairman Johnson, Ranking Member Shelby, and Members of the Committee, thank you for inviting me to appear before you today to talk about consumers' use of mobile financial services.

The evolution of new technologies that enable consumers to conduct financial transactions using mobile devices has the potential to affect their financial lives in important—but as of yet, not fully known—ways. For this reason, the Federal Reserve has been monitoring trends and developments in mobile financial services. By “mobile financial services,” I am really talking about two categories of activities. The first we call “mobile banking,” which is using your mobile device to interact with your financial institution, mostly doing things you could also do through more traditional means, like check your account balance or transfer money between accounts. The second we call “mobile payments,” which we define as making purchases, bill payments, charitable donations, or payments to other persons using your mobile device with the payment applied to your phone bill, charged to your credit card, or withdrawn directly from your bank account.

Beyond banking and payments, mobile devices have the potential to be useful tools in helping consumers track their spending, saving, investing, and borrowing, and in making financial decisions. Such technologies also hold the potential to expand access to mainstream financial services to segments of the population that are currently unbanked or underbanked. That said, the technologies are still new, and important concerns, such as consumers' expressions of unease about the security of these technologies, must also be addressed for consumers to feel confident adopting these new services.

To further our understanding of consumers' use of, and opinions about, such services, the Federal Reserve commissioned a survey late last year. Nearly 2,300 respondents completed the survey. This survey is among the first to integrate questions about using mobile devices for shopping and comparing products along with questions about using mobile devices for banking and payments. On March 14, 2012, the Federal Reserve released a report, based on these responses, titled “Consumers and Mobile Financial Services.”<sup>1</sup> My testimony today will draw from this report, which is attached to my written testimony.

Nearly 9 out of 10 adults in the United States have a mobile phone, and two-fifths of those phones are so-called “smartphones” with Internet connectivity. Among all mobile phone users, one out of five has used their phones to conduct some banking activity in the last 12 months. Those users with more traditional mobile phones, or so-called “feature phones,” access bank information via text messages, while smartphone users access their bank information by downloading their bank's application or via the bank's Internet site. Younger consumers, those below age 29, have readily adopted mobile banking, and make up almost 44 percent of all consumers surveyed who use such services. Adoption rates of mobile banking also differ by racial and ethnic background, with Hispanics and non-Hispanic blacks making up a disproportionate share of those who use mobile banking services. The most common transactions performed by users of mobile banking were checking account balances or checking recent transactions. Transferring money between accounts was another common transaction.

Of those consumers who had not adopted mobile banking, the primary reason given was that they felt their banking needs were being met through more traditional means. Security concerns were the second most-cited reason for not using mobile banking. Specifically, consumers expressed concerns about hackers gaining access to their phones and exposing their personal financial information. A little more than one-third of all mobile phone users reported that they do not know how secure mobile banking technology is for protecting their personal information, while an additional one-third rated the technology as unsafe. Nevertheless, among those con-

---

<sup>1</sup>The report is available at [www.federalreserve.gov/econresdata/mobile-device-report-201203.pdf](http://www.federalreserve.gov/econresdata/mobile-device-report-201203.pdf).

sumers with any type of mobile phone, but who are not currently using mobile banking, one out of ten expects to be using it within the next year.

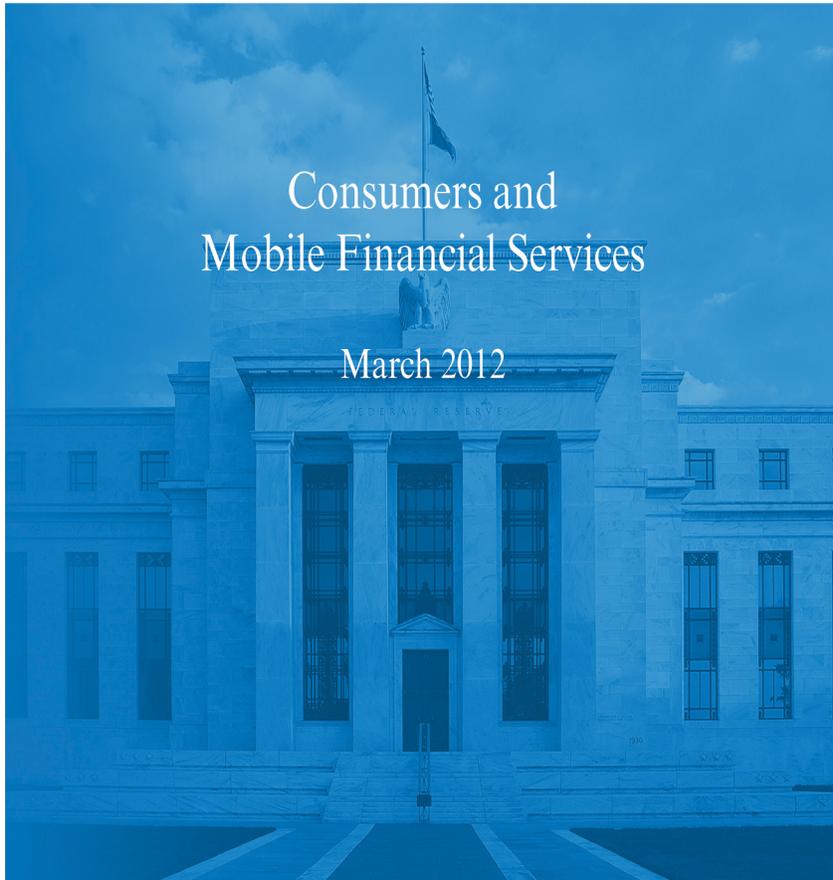
In addition to mobile banking, we asked about mobile payments, which I described earlier. Mobile payments are not yet as prevalent as mobile banking; one out of eight respondents reported making a mobile payment in the previous 12 months, and usually this involved paying a bill online via their mobile phone. Mobile payments are disproportionately used by consumers under age 45 and by Hispanics. Consumers who are not currently using mobile payments responded that they were concerned about the security of the technology, did not see any benefit from mobile payments, or found it easier to pay in other ways—for example, with cash or with a credit card.

Consumers who are “underbanked”—that is, those who have a bank account but who also use an alternative financial service provider such as a check casher, payday lender, auto-title lender, or payroll card—make significant use of mobile banking and mobile payments. Among this group, nearly three out of ten have used mobile banking, primarily to check their account balances. The underbanked are more likely than the general population to use mobile payments, with one out of six using payment services on their mobile devices. Those consumers who are unbanked also report using mobile financial services, generally in conjunction with a general purpose prepaid card or payroll card.

Let me give you a few examples from the report of how consumers reported using mobile financial services to make financial decisions. I stated earlier that the most frequent use of mobile banking was to check account balances. Of those consumers who use mobile banking, more than two-thirds reported that they checked their account balance or available credit before making a large purchase. Moreover, among the consumers that reported doing this, nearly six out of ten reported that they had decided not to buy an item because of the amount of money available in their account. As another example, some consumers reported setting up a text alert from their bank if their account balance was getting low; among those using this service, five out of six reported taking some action—transferring money into the account with the low balance, reducing spending, or making a deposit into the account—in response to receiving an alert. Consumers also reported using their mobile devices to browse product reviews or get pricing information while shopping.

More details on consumers’ use of mobile financial services are available in the report. Staff members in the Division of Consumer and Community Affairs expect to conduct additional analysis of the data in the months ahead. This should round out our understanding of these initial findings. For instance, some of the differences that we see based on ethnic or socioeconomic factors may be better understood when we examine how such factors interact with other characteristics of the respondents. We also anticipate that we may conduct periodic updates of the survey to monitor consumers’ experiences as the technology and business practices evolve.

Thank you again for inviting me to appear before you today. I would be happy to answer any questions you may have.





# Consumers and Mobile Financial Services

March 2012

To order additional copies of this or other Federal Reserve Board publications, contact:

Publications Fulfillment  
Mail Stop N-127  
Board of Governors of the Federal Reserve System  
Washington, DC 20551  
(ph) 202-452-3245  
(fax) 202-728-5886  
(e-mail) [Publications-BOG@frb.gov](mailto:Publications-BOG@frb.gov)

This and other Federal Reserve Board research into consumer topics is available online at  
[www.federalreserve.gov/econresdata/consumerresearch\\_publications.htm](http://www.federalreserve.gov/econresdata/consumerresearch_publications.htm).



## Preface

The survey and report were prepared by the Consumer Research Section of the Federal Reserve Board's Division of Consumer and Community Affairs (DCCA).

DCCA directs consumer-related functions performed by the Board and the Federal Reserve Banks, including conducting research on financial services policies practices and their implications for consumer

financial stability, community development, and neighborhood stabilization. For more information about DCCA, visit the Federal Reserve Board website at [www.federalreserve.gov](http://www.federalreserve.gov).

DCCA staff members Matthew B. Gross, Jeanne M. Hogarth, and Maximilian D. Schmeiser prepared this article.



## Contents

Executive Summary .....	1
<b>Introduction</b> .....	3
Trends in the Utilization of Mobile Banking and Payments .....	3
Potential Utilization for “Underbanked” and “Unbanked” Consumers .....	3
Younger Age Groups: Mobile Phone and Mobile Banking Adoption .....	4
Survey Background .....	4
<b>How Are Consumers Interacting with Financial Institutions?</b> .....	7
Online Banking .....	7
<b>Current Use of Mobile Banking and Payments</b> .....	9
Mobile Banking .....	9
Mobile Payments .....	11
Mobile Security .....	13
<b>Other Mobile Financial Services</b> .....	15
Shopping Behavior .....	15
Personal Financial Management and Budgeting .....	16
Unbanked and Underbanked .....	17
Conclusion .....	20
<b>Appendix 1: Survey of Consumers’ Financial Decisionmaking Using New Technologies—Questionnaire</b> .....	21
Banking Section .....	21
Mobile Banking Users .....	28
Mobile Payments Users .....	30
Non-Mobile Banking Users .....	32
Non-Mobile Payments Users .....	33
<b>Appendix 2: Consumer Responses to Survey Questionnaire</b> .....	47

## Executive Summary

Mobile devices have increasingly become tools that consumers use for banking, payments, budgeting, and shopping. This report presents findings from an online survey, conducted in December 2011 and January 2012, examining the use of mobile technology to access financial services and make financial decisions.

Key findings of the survey include

- **Mobile phones and mobile Internet access are in widespread use**

- 87 percent of the U.S. population has a mobile phone
- 44 percent of mobile phones are smartphones (Internet-enabled)
- 84 percent of smartphone users have accessed the Internet on their phone in the past week

- **The ubiquity of mobile phones is changing the way consumers access financial services**

- 21 percent of mobile phone owners have used mobile banking in the past 12 months
- 11 percent of those not currently using mobile banking think that they will probably use it within the next 12 months
- The most common use of mobile banking is to check account balances or recent transactions (90 percent of mobile banking users)
- Transferring money between accounts is the second most common use of mobile banking (42 percent of mobile banking users)

- **Mobile phones are also changing the way consumers make payments**

- 12 percent of mobile phone owners have made a mobile payment in the past 12 months

- The most common use of mobile payments was to make an online bill payment (47 percent of mobile payment users)

- 21 percent of mobile payment users transferred money directly to another person's bank, credit card, or Paypal account

- **Perceptions of limited usefulness and concerns about security are holding back the adoption of mobile financial services**

- The primary reason why mobile phone users had not yet adopted mobile banking was that they felt their banking needs were being met without the use of mobile banking (58 percent)
- Concerns about the security of the technology were the primary reason given for not using mobile payments (42 percent) and the second most common reason given for not using mobile banking (48 percent)

- More than a third of mobile phone users who do not use mobile payments either don't see any benefit from using mobile payments or find it easier to pay with another method

- **The "underbanked" make significant use of mobile financial services**

- The underbanked make comparatively heavy use of both mobile banking and mobile payments, with 29 percent having used mobile banking and 17 percent having used mobile payments in the past 12 months
- 62 percent of the underbanked who use mobile payments have used it to pay bills
- 10 percent of the completely unbanked report using mobile banking in the past 12 months, and 12 percent have made a mobile payment

## Introduction

Mobile phones have clearly become ubiquitous and a standard aspect of daily life for many American consumers in the last decade. Ongoing innovations in mobile finance show some potential to change the way consumers conduct financial transactions by offering consumers new services. Yet, many people remain skeptical of the benefit of mobile financial services and the level of security provided along with such services.

To further understanding of these developments and consumers' usage of and attitudes towards mobile financial services, the Board conducted a consumer survey in late 2011 and early 2012.

### Trends in the Utilization of Mobile Banking and Payments

A number of new services allow consumers to obtain financial account information and conduct transactions with their financial institution ("mobile banking") and others allow consumers to make payments, transfer money, or pay for goods and services ("mobile payments").

As the market share of Internet-enabled smartphones continues to grow, the utilization of mobile banking and mobile payment technologies also increases.<sup>1</sup> As of March 2011, nearly one out of every five Americans with both a bank account and a mobile phone has used their phone to view account balances, receive account alerts, and conduct banking with their financial institution in the past 90 days.<sup>2</sup>

<sup>1</sup> The Pew Research Center reports that 35 percent of American adults owned a smartphone as of May 2011. Pew Internet study, 2011, *35% of American Adults Own a Smartphone* ([http://pewinternet.org/~media/Files/Reports/2011/PIP\\_Smartphones.pdf](http://pewinternet.org/~media/Files/Reports/2011/PIP_Smartphones.pdf)).

<sup>2</sup> In its July 2011 report on smartphone banking security (based on a March 2011 survey), Javelin Strategy and Research finds that 19 percent of U.S. consumers are using mobile banking. Javelin, 2011, "Smartphone Banking Security: Mobile Banking Utilization Stalls on Consumer Fears."

Although mobile payments have been adopted more slowly by consumers in the U.S. than in many other countries, these services may become more popular over the coming years as the technology evolves and if the services become more widely accepted as a form of payment. In September 2011, for example, Google launched the Google Wallet service, which allows consumers to use smartphones equipped with a near field communication (NFC) chip to make "tap payments" at any retailer accepting MasterCard Pay-Pass. Besides Google, many other firms—including mobile phone carriers, credit card issuers, and payment networks—are investing in mobile wallet technology. As the number of phones equipped with NFC increases, mobile payments may also increase.

Consumers respond to timely financial incentives and emotional appeals. Recent survey data show that some consumers view mobile payments as time-saving and convenient while providing them with increased access to, and control of, their finances. Despite these positive mobile finance attributes and perceptions, consumers also remain concerned about the cost and the security risks inherent in mobile financial transactions.<sup>3</sup>

### Potential Utilization for "Underbanked" and "Unbanked" Consumers

Mobile phone use is high among younger generations, minorities, and those with low levels of income—groups that are prone to be unbanked or underbanked. Mobile banking and mobile payments have the potential to expand financial access to the unbanked and underbanked by reducing transaction costs and increasing the accessibility of financial products and services.

<sup>3</sup> Javelin, 2011, *Smartphone Banking Security: Mobile Banking Utilization Stalls on Consumer Fears*.

A significant number of Americans do not have a bank account of any kind, and many make regular use of alternative financial services such as payday loans, check cashers, rent-to-own services, money orders, or pawn shops. A 2009 study by the Federal Deposit Insurance Corporation (FDIC) found that 8 percent of Americans had no checking or savings account, and thus were defined as unbanked.<sup>4</sup> An additional 18 percent had a bank account but had used an alternative financial service at least once per year and so were classified as underbanked.

While there remains a digital divide in computer Internet access across the socioeconomic spectrum, this divide does not hold true for mobile phone access. The 2011 Pew Internet study showed that 83 percent of American adults have a mobile phone, and 35 percent have a smartphone that can access the Internet. Moreover, adoption of mobile phones is actually higher among minorities, as 89 percent of non-Hispanic blacks and 86 percent of Hispanics own a mobile phone.

Indeed, minorities are also more likely to own a smartphone than non-Hispanic whites, with 44 percent of both non-Hispanic blacks and Hispanics owning a smartphone compared with 30 percent of non-Hispanic whites. While mobile phone and smartphone adoption is less prevalent at lower levels of income, approximately 75 percent of U.S. adults in households earning less than \$20,000 per year have a mobile phone of some type, and 20 percent have a smartphone.<sup>5</sup>

### Younger Age Groups: Mobile Phone and Mobile Banking Adoption

Unsurprisingly, mobile phone adoption is highest for younger age groups: only 5 percent of individuals ages 18 to 24 do not have a mobile phone, and 49 percent have a smartphone. In contrast, 44 percent of those ages 65 and over do not have a mobile phone, and only 11 percent have a smartphone.<sup>6</sup>

Furthermore, and perhaps more surprisingly, a recent survey by the Center for Financial Services Innova-

tion (CFSI) shows that individuals under the age of 25 are increasingly underbanked—some as a matter of choice—and appear comfortable with alternative financial services.<sup>7</sup> Given the prevalence of mobile phone usage among young individuals, minorities, and low-income families—groups most likely to be unbanked or underbanked—there is potential for mobile financial services to help integrate these individuals into the financial mainstream.

### Survey Background

In consultation with a mobile financial services advisory group made up of key Federal Reserve System staff with relevant consumer research backgrounds, the Consumer Research Section in the Federal Reserve Board's Division of Consumer and Community Affairs designed a survey instrument to examine consumers' usage of and attitudes towards mobile phones and mobile financial services.

The survey was administered by Knowledge Networks, an online consumer research company, on behalf of the Board. The survey was conducted using a sample of adults ages 18 and over from KnowledgePanel®, a proprietary, probability-based web panel of more than 50,000 individuals from randomly sampled households; the sample was designed to be representative of the U.S. population. After pretesting, the data collection for the survey began on December 22, 2011 and concluded on January 9, 2012. The 2,290 respondents completed the survey in approximately 15 minutes (median time).

The number of respondents sampled and participating in the survey, and the survey completion rates, are presented in table 1. A total of 3,382 e-mail solicitations to participate in the survey were sent out to the KnowledgePanel, and 2,290 individuals completed the survey fully (a "cooperation rate" yield of 68 percent). To enhance the cooperation rate, Knowledge

<sup>7</sup> Center for Financial Services Innovation (CFSI), 2010, *Financial First Encounters: An Examination of the Fractured Financial Landscape Facing Youth Today* ([http://cfsinnovation.com/sites/default/files/first\\_encounters\\_white\\_paper\\_12\\_16\\_0.pdf](http://cfsinnovation.com/sites/default/files/first_encounters_white_paper_12_16_0.pdf)).

<sup>4</sup> Federal Deposit Insurance Corporation, 2009 *Survey of Unbanked and Underbanked Households* ([www.fdic.gov/householdsurvey/full\\_report.pdf](http://www.fdic.gov/householdsurvey/full_report.pdf)).

<sup>5</sup> Pew Internet study, 2011, *35% of American Adults Own a Smartphone* ([http://pewinternet.org/~media/Files/Reports/2011/PIP\\_Smartphones.pdf](http://pewinternet.org/~media/Files/Reports/2011/PIP_Smartphones.pdf)).

<sup>6</sup> *Ibid.*

Table 1. Key survey response statistics: Main interview

Number sampled for main survey	Qualified completes	Cooperation rate
3,382	2,290	68%

Networks sent e-mail reminders to non-responders on days three and six of the field period.

The responses to all the survey questions are presented in Appendix 2 in the order in which they were asked of respondents. A table of summary statistics for the respondent demographics is also included as table B.87. Beginning at table B.88, cross-tabulations are presented of consumers' use of online banking, telephone banking, mobile banking, and mobile payments by age, race, gender, education, and income.

The following sections of this report summarize key findings from the Knowledge Networks survey of consumers, with a focus on how consumers are using mobile phones to conduct their banking, make payments, enhance information gathering while shopping, and manage their finances. All data were weighted to yield estimates for the U.S. population. Only questions pertaining to these topics are discussed in the report; however, the complete survey questionnaire and the results of the entire survey are summarized in Appendix 1 and Appendix 2.

## How Are Consumers Interacting with Financial Institutions?

Survey respondents were asked a set of screening questions that covered whether or not they had a bank account, access to the Internet, and ownership of mobile phones or smartphones. Survey responses indicate that the majority of American consumers use some form of technology to interact with their financial institution.

As shown in **figure 1**, of those consumers with regular Internet access and a bank account, 68 percent used online banking in the past 12 months. Telephone banking is the second most commonly used method of accessing financial services, with 33 percent of banked consumers reporting that they used it in the past 12 months. Mobile banking and mobile payments are the least common methods of accessing financial services, as just over a fifth of respondents with mobile phones and a bank account report using mobile banking and only 11 percent report using mobile payments in the past 12 months.

However, as discussed in the following section, mobile banking access appears to be gaining traction with consumers and is likely to overtake telephone banking access in the next couple of years (as measured by consumers' expectations regarding their future use of the technology).

### Online Banking

Three out of ten respondents (30 percent) who use online banking are between ages 30 and 44, while 20 percent of the online banking users are age 60 and older (see tables B.88, B.91, B.94, B.97, and B.100 in Appendix 2). Online banking users are predominantly non-Hispanic whites (73 percent), while Hispanics and non-Hispanic blacks comprise about 12 percent and 8 percent of the online banking community, respectively.

Online banking users are split evenly among men and women. Use of online banking is generally unrelated to household income, with the share of online banking users by income category corresponding to their share of the population. Exceptions occurred at the tails of the income distribution, with those individuals earning less than \$25,000 per year being significantly less likely to use online banking than their share of the population would suggest, while those individuals earning more than \$100,000 per year being significantly more likely to use online banking than their share of the population would suggest. Level of education and use of online banking have a linear relationship, with online banking use increasing as education level increases: individuals with a

Figure 1. Usage of different means of accessing banking services



Note: The denominator varies across services due to question screening.

bachelor's degree or higher account for 39 percent of individuals with a bank account. online banking users relative to 30 percent of indi-

## Current Use of Mobile Banking and Payments

### Mobile Banking

The Federal Reserve survey defines mobile banking as “using a mobile phone to access your bank account, credit card account, or other financial account. Mobile banking can be done either by accessing your bank’s web page through the web browser on your mobile phone, via text messaging, or by using an application downloaded to your mobile phone.”

A significant number of mobile phone users have already adopted mobile banking. Nearly 21 percent of mobile phone users in the survey report that they used mobile banking in the past 12 months.<sup>8</sup> Moreover, among those consumers who do not currently use mobile banking, 11 percent report that they will “definitely” or “probably” use mobile banking in the next 12 months. An additional 17 percent of those who report that they are unlikely to use mobile banking in the next 12 months report that they will “definitely” or “probably” adopt mobile banking at some point. Adding all these respondents together would imply peak adoption of 42 percent of all mobile phone owners.<sup>9</sup> As smartphone users are more likely to adopt mobile banking than non-smartphone users, increasing smartphone adoption should further fuel mobile banking adoption.

<sup>8</sup> There is a wide range of estimates of mobile banking adoption. comScore estimates that 13.9 percent of all mobile phone users had adopted mobile banking as of Q2 2011. Javelin estimated that 19 percent of mobile phone users had adopted mobile banking as of March 2011 (Smartphone Banking Security Report); however, the firm subsequently reports that mobile banking adoption jumped to 30 percent as of June 2011 (comScore, 2011, *Mobile Banking Financial Institution Scorecard*).

<sup>9</sup> The denominator for each of the questions on mobile banking adoption varies, thus the potential adoption rate is less than the sum of the percentages of respondents who indicate that they have or will adopt mobile banking. There are a total of 2,002 mobile phone users in our survey; 418 are current users of mobile banking, 182 report that they are likely to use mobile banking in the next 12 months, and 246 report that they will likely use mobile banking at some point in the future (for a total of 846 potential users, or 42 percent of all 2,002 mobile phone users).

Use of mobile banking appears to be highly correlated with age (table 2), as individuals between ages 18 and 29 account for approximately 44 percent of mobile banking users, relative to 22 percent of mobile phone users. Conversely, individuals age 60 and over account for only 6 percent of all mobile banking users, while at the same time they represent 24 percent of all mobile phone users.

Non-Hispanic black and Hispanic users show a disproportionately high rate of adoption of mobile banking (table 3), at 16 percent and 17 percent of all mobile banking users relative to 11 percent and 13 percent of mobile phone users, respectively. Meanwhile, mobile banking users are split evenly between males and females, and use of mobile banking is generally unrelated to household income (table 4), with

**Table 2. Use of mobile banking in the past 12 months by age**  
Percent, except as noted

Age categories	Yes	No	Total
18-29	43.5	16.8	22.4
30-44	35.7	24.7	27
45-59	14.7	30.2	26.9
60+	6.1	28.4	23.7
<b>Number of respondents</b>	<b>372</b>	<b>1,626</b>	<b>1,998</b>

Note: This is table B.89 in Appendix 2.

**Table 3. Use of mobile banking in the past 12 months by race**  
Percent, except as noted

Race/ethnicity	Yes	No	Total
White, Non-Hispanic	60.3	71.5	60.2
Black, Non-Hispanic	16.2	10	11.3
Other, Non-Hispanic	5.2	5.8	5.6
Hispanic	17.1	11.6	12.8
2+ Races, Non-Hispanic	1.2	1.1	1.2
<b>Number of respondents</b>	<b>372</b>	<b>1,626</b>	<b>1,998</b>

Note: This is table B.92 in Appendix 2.

**Table 4. Use of mobile banking in the past 12 months by income group**  
Percent, except as noted

Income group	Yes	No	Total
Less than \$25,000	12.8	19.9	18.4
\$25,000–\$39,999	19	16.6	17.1
\$40,000–\$74,999	27.5	26.5	26.7
\$75,000–\$99,999	12.9	14	13.8
\$100,000 or greater	27.9	22.9	24
<b>Number of respondents</b>	<b>372</b>	<b>1,626</b>	<b>1,998</b>

Note: Table B.101 in Appendix 2.

the share of mobile banking users by income category corresponding to their share of the mobile phone user population. As with online banking, exceptions occurred at the tails of the income distribution, with those individuals earning less than \$25,000 per year being significantly less likely to use mobile banking than their share of the mobile phone

**Table 5. Use of mobile banking in the past 12 months by education group**  
Percent, except as noted

Education (categorical)	Yes	No	Total
Less than high school	5.5	12.1	10.7
High school	21.5	31.8	29.6
Some college	39	27.4	29.8
Bachelor's degree or higher	34	28.8	29.9
<b>Number of respondents</b>	<b>372</b>	<b>1,626</b>	<b>1,998</b>

Note: Table B.98 in Appendix 2.

user population would suggest, while those individuals earning more than \$100,000 per year being significantly more likely to use mobile banking than their share of the mobile phone user population would suggest. Mobile banking is highly correlated with education (table 5): 73 percent of all mobile banking users have at least some college education, but this education group represents only 60 percent of all mobile phone users.

By far, checking financial account balances or transaction inquiries were the most common mobile banking activity, with 90 percent of mobile banking users having performed this function in the past 12 months (figure 2). Less prevalent activities were transferring money between accounts (42 percent) or receiving a text message alert from a bank (33 percent). Less frequently used mobile banking functions include making online bill payments from a bank account (26 percent), locating an in-network ATM (21 percent), and depositing a check by phone (11 percent). Lastly, mobile investment management is utilized by only 2 percent of mobile banking users. Many mobile banking users appear to be making use of their banks' mobile applications, as 48 percent have installed such an application on their phones.

Consumers report using mobile banking up to 60 times per month; however, the median number of mobile banking transactions is four or five times in a typical month.

Of the consumers who use mobile banking, many appear to be quite satisfied with their experiences, as



62 percent report being “very satisfied” with their experiences, and another 32 percent report being “somewhat satisfied” with their experiences.

Among those consumers with mobile phones who do not currently use mobile banking, the top two reasons for not using the service are that they believe their banking needs are met without mobile banking (58 percent) and that they are concerned about security (48 percent) (figure 3). Less commonly cited reasons include a lack of trust in the technology to process transactions properly (22 percent), the high cost of data access on mobile phones (18 percent), and the small size of the mobile phone screen (17 percent).

Consumers who express concerns about the security of mobile banking are concerned with hackers gaining access to their phone remotely (54 percent), losing their phone or having it stolen (19 percent), and experiencing data interception by a third party (18 percent). If these concerns were addressed, many non-users would be willing to adopt mobile banking.

Moreover, the potential uses of mobile banking by those who have yet to adopt it largely mirror those of current users. The majority is interested in checking financial account balances or recent transactions (55 percent), while fewer are interested in receiving text message alerts from their bank (30 percent), transferring money between accounts (25 percent), or making bill payments (24 percent).

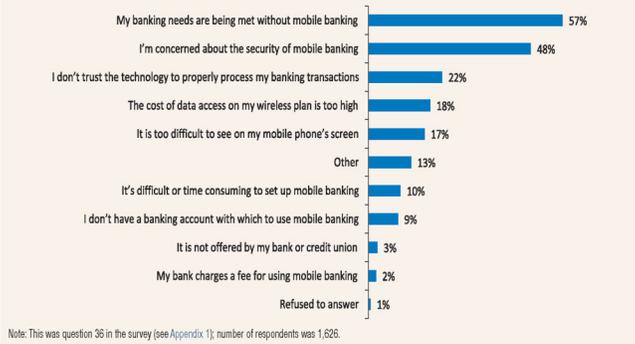
### Mobile Payments

The Federal Reserve survey defined mobile payments as “purchases, bill payments, charitable donations, payments to another person, or any other payments made using a mobile phone. Mobile payments can be used by accessing a web page through the web browser on your mobile device, by sending a text message (SMS), or by using a downloadable application on your mobile device. The amount of the payment may be applied to your phone bill (for example, Red Cross text message donation), charged to your credit card, or withdrawn directly from your bank account.”

Consumers were less likely to adopt mobile payments than mobile banking, with only 12 percent of mobile phone users reporting that they made a mobile payment in the past 12 months. Mobile payment users also perform a narrower set of transactions than mobile banking users, with the most common activity being payment of bills (47 percent), followed by making online purchases (36 percent) and transferring money directly to another person (21 percent). All other transactions (e.g., receiving a payment, texting to make a charitable donation) are used by less than 10 percent of those making mobile payments.

Mobile payments are disproportionately used by younger consumers (table 6). Individuals age 18 to 29 account for 37 percent of mobile payment users relative to 22 percent of all mobile phone users, while

Figure 3. What are the main reasons you have decided not to use mobile banking?



**Table 6. Use of mobile payments in the past 12 months by age**

Percent, except as noted

Age categories	Yes	No	Total
18-29	37.3	20.3	22.4
30-44	35.9	25.6	26.9
45-59	16.9	28.5	27
60+	10	25.7	23.7
<b>Number of respondents</b>	<b>213</b>	<b>1,780</b>	<b>1,993</b>

Note: This is table B.90 in Appendix 2.

individuals age 30 to 44 account for a further 36 percent of mobile payment users relative to 27 percent of all mobile phone users. Hispanic consumers are active users of mobile payments, accounting for approximately 21 percent of all mobile payment users relative to 13 percent of all mobile phone users (table 7). In contrast, non-Hispanic whites are proportionally less likely to use mobile payments, as they make up 58 percent of mobile payment users but are 69 percent of mobile phone users. Almost 13 percent of non-Hispanic blacks use mobile payments, which is comparable to their 11 percent share of the mobile phone user population. Females are slightly more likely to use mobile payments than males, accounting for 55 percent of all users (table 8). Income does not play a role in mobile payment use, as each income group represents roughly the same percentage as it does in the overall mobile phone user sample (table 9). Similarly, mobile payment use by education level is roughly proportionate to its representation in the mobile phone user population (table 10).

Consumers use a variety of methods to make mobile payments, but the most common method is to input a credit card, debit card, or prepaid card number into a mobile phone (66 percent). Other mobile payment techniques used by consumers include making pay-

**Table 7. Use of mobile payments in the past 12 months by race**

Percent, except as noted

Race/ethnicity	Yes	No	Total
White, Non-Hispanic	58.3	70.8	69.3
Black, Non-Hispanic	12.9	10.9	11.2
Other, Non-Hispanic	7.1	5.4	5.6
Hispanic	20.9	11.6	12.8
2+ Races, Non-Hispanic	0.9	1.2	1.2
<b>Number of respondents</b>	<b>213</b>	<b>1,780</b>	<b>1,993</b>

Note: This is table B.93 in Appendix 2.

**Table 8. Use of mobile payments in the past 12 months by gender**

Percent, except as noted

Sex	Yes	No	Total
Female	55	52.7	53
Male	45	47.3	47
<b>Number of respondents</b>	<b>213</b>	<b>1,780</b>	<b>1,993</b>

Note: This is table B.95 in Appendix 2.

ments directly from a bank account (45 percent); using Google Wallet, Paypal, or iTunes (22 percent); or adding a payment to a mobile phone bill (8 percent).

Consumers use mobile payment services less frequently than they do mobile banking services. The median number of mobile payments in a typical month is one. Although some respondents reported making as many as 24 mobile payments per month, fewer than 7 percent of respondents make more than five payments in a typical month.

As with mobile banking, users of mobile payments appear to be quite satisfied with their experiences:

**Table 9. Use of mobile payments in the past 12 months by income group**

Percent, except as noted

Income group	Yes	No	Total
Less than \$25,000	19.1	18.5	18.5
\$25,000-\$39,999	20.6	16.7	17.2
\$40,000-\$74,999	23	27.2	26.7
\$75,000-\$99,999	11.7	14	13.7
\$100,000 or greater	25.6	23.6	23.9
<b>Number of respondents</b>	<b>213</b>	<b>1,780</b>	<b>1,993</b>

Note: This is table B.102 in Appendix 2.

**Table 10. Use of mobile payments in the past 12 months by education group**

Percent, except as noted

Education (categorical)	Yes	No	Total
Less than high school	7.2	11.2	10.7
High school	27.9	29.9	29.7
Some college	37	28.7	29.7
Bachelor's degree or higher	27.9	30.1	29.9
<b>Number of respondents</b>	<b>213</b>	<b>1,780</b>	<b>1,993</b>

Note: This is table B.99 in Appendix 2.

55 percent report being “very satisfied” with their experiences and 33 percent report being “somewhat satisfied” with their experiences.

Although security is the dominant reason why individuals do not use mobile payments (42 percent), there are many consumers who do not see any value in mobile payments; 36 percent report that it is easier to pay with other methods, and 37 percent report that they do not see any benefit from using mobile payments (figure 4). Other reasons for not using include the lack of necessary features on a phone (31 percent) and a lack of trust in the technology to properly process payments (20 percent).

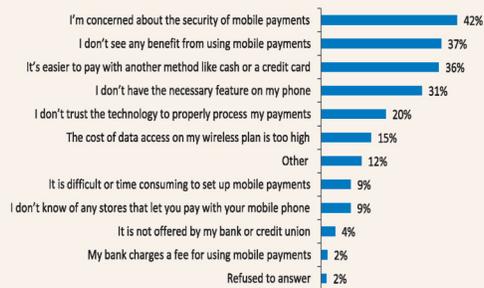
If the concerns of non-users of mobile payments were addressed, those consumers express that they would have an interest in using mobile payments for a variety of activities. In particular, 34 percent report that they would pay bills online using their phone, 28 percent would receive coupons on their phone, and 22 percent say they would receive location-based offers or buy goods and services online. Making person-to-person payments is listed by 17 percent of respondents as a preferred mobile payment activity; the same percentage expresses a similar sentiment for using a mobile phone as the payment mechanism at a cash register or to use a phone as a “virtual wallet.” Consumers also express some interest in using mobile payments to transfer money to friends or relatives in other countries (7 percent).

## Mobile Security

Two major impediments to consumers’ adoption of mobile banking and mobile payment technologies are (1) concerns about security and (2) the possibility of hackers remotely accessing consumers’ phones. Consumers’ beliefs about whether mobile banking or mobile payment technologies are secure is correlated with their use of these technologies. Consumers who use mobile banking or mobile payments are more likely to report that it is a secure process than those who do not use mobile banking or mobile payments. For example, when consumers were asked to rate the security of text messages for mobile banking, those who are mobile banking users rate the service “very safe” (18 percent) or “somewhat safe” (42 percent). In contrast, 38 percent of non-users of mobile banking report that they “don’t know” whether or not text messages for mobile banking are safe, while only 6 percent rate the service “very safe” and 27 percent rate it “somewhat safe.”

The dichotomy between users and non-users of mobile banking is even more pronounced when asked about the overall security of mobile banking for protecting personal information. Two-fifths of non-users report that they do not know if it is secure, while 13 percent of this group rate mobile banking “very insecure” and 23 percent rate the service “somewhat insecure.” Mobile banking users, however, rate mobile banking as “very safe” (18 percent) or “somewhat safe” (56 percent) in maintaining their personal information.

Figure 4. What are the main reasons why you have not used mobile payments?



Note: This was question 36 in the survey (see Appendix 1); number of respondents was 1,780.

## Other Mobile Financial Services

There appears to be widespread interest among mobile phone users in expanding how they use mobile technology to access financial services, despite the Federal Reserve survey finding that only 21 percent of respondent mobile phone users have adopted mobile banking and only 12 percent of respondents have adopted mobile payments.

Consumers were asked to select the types of activity they would be interested in performing with their mobile phones assuming the function were made available to them (figure 5). Nearly one-half (48 percent) of consumers in the survey express an interest in using their phone to compare prices while shopping. Similarly, one-third indicate that they would like to use their mobile phones to receive location-based offers and promotions, and 31 percent indicate that they would like to receive and manage discount offers and coupons. Consumers also report that they would use their mobile phones to manage their personal finances, as 31 percent indicate that they would like to use their mobile phones to track their finances on a daily basis.

Consumers in the survey have a limited interest in using their mobile phone as a “mobile wallet”: 25 percent indicate they would like to use their mobile phone to pay at the point of sale. Given the current mobile payment adoption rate of 12 percent, this would double the use of mobile payments. One fourth indicate they would use it as a membership card, and 21 percent indicate they would use it to organize and track gift cards, loyalty points, and reward points. In a related potential application of mobile technology, 23 percent of consumers indicate that they would like to use their mobile phones as a form of photo identification.

### Shopping Behavior

The adoption of smartphones with barcode scanning software and Internet access has the potential to substantially alter consumer behavior in the retail environment. With this technology, consumers can quickly and easily compare prices across retailers

Figure 5. Would you like to use your mobile phone for any of the following purposes, assuming they were made available to you?



Note: This was question 46 in the survey (see Appendix 1); number of respondents was 2,002.

while in store or online, or locate an item that is out of stock.

Consumers can also browse product reviews or get product specifications with little effort. Thus, consumers may become better informed about the products they purchase and find lower prices; however, the ease with which these tasks can be performed might also encourage impulse buying.

Consumers already make significant use of the Internet to inform their major purchases. A majority of respondents (58 percent) indicate that they comparison-shop online, and the same percentage say they look at product reviews before making a large purchase while at a retail store. Even though security concerns may make consumers wary of mobile devices as the payment mechanism for point-of-sale purchases, the technology can enable shopping and comparisons of products and services. About one in eight (16 percent) mobile phone users report using their mobile phone for online shopping, and nearly one-fifth of consumers with mobile phones (19 percent) say that they use their mobile phone to comparison shop while at a retail store.

Despite the relative novelty of barcode scanning applications, the Federal Reserve survey found that 12 percent of mobile phone users report using a barcode scanning application for price comparisons. One in six (16 percent) mobile phone users report using their mobile phone to browse online shopping reviews while in the store.

Many consumers who use their mobile phone to comparison-shop report that they altered their decisions as a result: 65 percent who have comparison-shopped in a store report that they changed where they made a purchase after comparing prices, and 77 percent report that they changed what they purchased as a result of reading product reviews on their mobile phone while at a retail store.

Meanwhile, as a growing number of retailers develop their capabilities in the mobile space, opportunities will arise for the use of mobile advertisements and offers. Thirty-seven percent of consumers in the survey report signing up for coupons or special offers by e-mail from retail stores in the past 12 months, and 73 percent of these consumers report having made a purchase as a result of these promotions. Moreover, 28 percent of all consumers report signing up with an online coupon or offer site such as Groupon or Living Social.

## Personal Financial Management and Budgeting

Some consumers appear to be actively managing their finances using their computer and some form of personal financial management (PFM) tool. For the purposes of this survey, the Federal Reserve defined a PFM tool as a “program or website used to track your household finances (e.g., Quicken, Mint.com, Excel, or a website provided by a bank).” Slightly more than one in five consumers (21 percent) report that they, or someone in their household, use a program or website to track their household finances. Most consumers who track their finances are long-time users—42 percent report using the program or website for more than five years. The median consumer uses PFM tools about five times a month (just about once a week).

Access on a mobile phone to information about financial accounts has the potential to shape consumers’ financial decisions. For example, 67 percent of mobile banking users report using their mobile phone to check account balances or available credit before making a large purchase in the past 12 months. Of those who checked their balance or available credit, 59 percent report that they decided not to buy an item because of the amount of money in their bank account or the amount of available credit.

Furthermore, some mobile phones not only allow their users to access financial accounts but also serve as PFM tools. For example, 7 percent of mobile phone users report using their mobile phone to track purchases and expenses. Among this group, 38 percent use a mobile application for expense tracking, 10 percent use a spreadsheet, 47 percent use the web browser to access a website, 12 percent send text messages, and 21 percent take notes in a notepad or word processor.

Consumers can take advantage of other financial management tools on their mobile phones, such as text alerts, to make smarter financial decisions. Alerts, reminders, and similar services provided by banks are meant to encourage positive consumer behaviors and, given the positive response to low-balance alerts, it seems that text message notices are an effective tool for encouraging consumers to engage in better financial behaviors.

One-third of mobile banking users indicate that they receive text message alerts from their bank and, out of this group, 66 percent receive “low-balance alerts” (figure 6). Nearly all report taking some action in response to getting a low-balance text alert from their bank: transferring money into the account with the low-balance (58 percent), reducing their spending (41 percent), or depositing additional money into the account (16 percent) (figure 7). Almost one-third of text message bankers (31 percent) indicate that they receive “payment due alerts,” and 3 percent indicate that they receive “savings reminders.”

### Unbanked and Underbanked

As previously discussed, mobile technologies offer an opportunity to draw the unbanked and underbanked into the mainstream financial system by providing easily accessible and low-cost financial services.

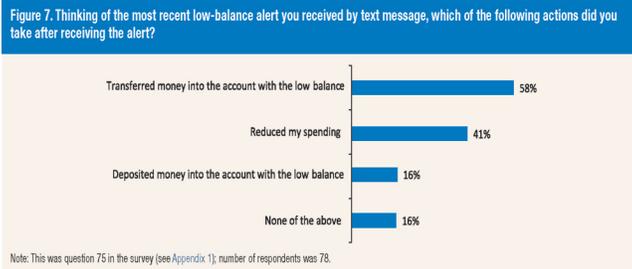
### Who Are the Unbanked and Underbanked?

For purposes of this report, an underbanked consumer is defined as a respondent who has a checking, savings, or money market account, but who also uses an alternative financial service such as auto title lending, payday loans, a check-cashing service, or a payroll card. An unbanked consumer is defined as someone who does not currently have a checking, savings, or money market account (see box 1).

The proportion of respondents who report being unbanked or underbanked in this survey closely tracks that found in previous national studies. In this study, about 11 percent of the U.S. adult population is currently unbanked, compared with approximately 8 percent according to the 2009 Federal Deposit Insurance Corporation (FDIC) National Survey of Unbanked and Underbanked Households and 8 percent according to the Federal Reserve’s 2007 Survey of Consumer Finances (SCF).<sup>10</sup>

Results indicate that a further 11 percent of the U.S. population is underbanked. This rate is well below the 18 percent underbanked rate found in the FDIC study; however, the definition of underbanked here is more narrow than the FDIC’s definition, as the latter includes use of services such as money orders when classifying an individual as underbanked.

<sup>10</sup> Bucks, Brian K., Arthur B. Kennickell, Traci L. Mach and Kevin B. Moore, 2009, “Changes in U.S. Family Finances from 2004 to 2007: Evidence from the Survey of Consumer Finances,” *Federal Reserve Bulletin* ([www.federalreserve.gov/pubs/bulletin/2009/pdf/scf09.pdf](http://www.federalreserve.gov/pubs/bulletin/2009/pdf/scf09.pdf)).



**Box 1. Alternatives to Traditional Banking and Financial Services**

The survey included other questions on consumers' use of financial products, consumer financial behaviors, and consumer attitudes. Among those questions were ones on alternative financial services; results are reported here because of the general interest in these topics among consumer educators and community development professionals.

Over the past several decades, new financial products and services have arisen to meet the needs of consumers who may not have had their financial needs met by mainstream financial institutions, or who wanted an alternative to mainstream financial institutions.

The spreading availability and use of payday lenders, check cashers, and prepaid debit cards are prime examples of this trend.

These products and services charge fees and effective interest rates that, in some cases, can impose a significant burden on the finances of consumers and can be detrimental to consumers' long-term financial well-being.

Payday lenders typically charge consumers fees ranging from 15 to 20 percent of the loan amount for a two-week loan, which translates into an Annual Percentage Rate (APR) ranging from 390 percent to 520 percent.<sup>1</sup>

<sup>1</sup> Avery, Robert B. and Katherine A. Samolyk. 2011. *Payday Loans versus Pawn Shops: The Effects of Loan Fee Limits on Household Use*. Working Paper ([www.ftbcl.org/community/conferences/2011ResearchConference/docs/2-avery-paper.pdf](http://www.ftbcl.org/community/conferences/2011ResearchConference/docs/2-avery-paper.pdf)).

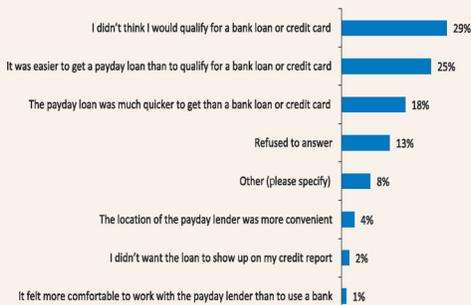
Among the various alternative financial products and services, use of prepaid cards is the most common in our sample—more than half (55 percent) of the respondents report using some type of prepaid card. About one out of seven respondents (15 percent) use a general purpose prepaid card, 5 percent have a government provided prepaid card, and 2 percent have a payroll card.

**Why Consumers Use Payday Lenders**

Eleven percent of respondents in our sample report that they or their partner/spouse have used a payday loan, but only 5 percent report having done so in the past 12 months. As shown in figure A, the main reasons for using payday loans or advances are perceptions that the borrower would not qualify for a bank loan or credit card (29 percent), that payday loans are easier to get than a bank loan or credit card (25 percent), and that payday loans are quicker to receive than other loans (18 percent). Few respondents indicate that the reason for using the payday lender is convenience (4 percent) or level of comfort with banks (1 percent).

Besides payday lenders and prepaid cards, the use of the other types of alternative financial services was quite rare in our sample. Only 4 percent of the overall sample reports having used a check-cashing service, auto title loan, or layaway loan in the past 12 months.

**Figure A. What was the main reason for using a payday loan or payday advance service rather than a bank loan or credit card?**



Note: This was question 6 in the survey (see Appendix 1); number of respondents was 223.

**Why Are Consumers Unbanked and Underbanked?**

From this survey, the reasons reported for being unbanked largely mirror those found in the 2007 SCF. The most commonly cited reason is a general dislike of dealing with banks (24 percent) (figure 8). Meanwhile, 23 percent report that they do not write enough checks to justify owning an account, and 13 percent indicate that the fees and service charges on an account are too high. A further 10 percent of the unbanked report that banks would not allow them to open an account.

This order of response frequency for why consumers remain unbanked tracks that found in the 2007 SCF, and the magnitudes are nearly identical. For example, 25 percent of unbanked respondents to the SCF report that they do not have a checking account because they do not like dealing with banks, and 19 percent report that they don't write enough checks to make it worthwhile.

**Mobile Device Use by the Unbanked and Underbanked**

Although 11 percent of all individuals are unbanked, they are not necessarily "unphoned." Among individuals who are unbanked, 64 percent have access to a mobile phone and 18 percent have access to a smartphone. More remarkably, 91 percent of the underbanked have a mobile phone and 57 percent

have a smartphone—rates far above those for the overall population.

**The Unbanked and Mobile Banking**

The utilization of mobile banking among the unbanked is low, with only 10 percent reporting its use in the past 12 months. Although the concept of an unbanked mobile banking user seems counterintuitive, 32 percent of unbanked individuals do, nevertheless, report using a debit card or check card in the past 12 months. Recall that our definition of mobile banking used here includes "using a mobile phone to access your bank account, credit card account, or other financial account [emphasis added]." Respondents may be referring to another financial account, such as a payroll card or prepaid card, often marketed as a "debit" card.

Additionally, 19 percent of the unbanked report using a general purpose prepaid card in the past 12 months, and 9 percent report using a major credit card in the past 12 months. Mobile payment adoption among the unbanked is 12 percent, which is approximately the same as in the overall population. Given the sample size of the survey, the number of individuals who are unbanked and use mobile financial services is fewer than 20, which prevents detailed analysis of their behavior.

**The Underbanked and Mobile Financial Services**

The underbanked population makes substantial use of mobile financial services. Almost 29 percent of the underbanked with mobile phones report using mobile banking in the past 12 months, while 17 percent report using mobile payments.

As with all other consumers, the primary use for mobile banking among the underbanked is to check account balances, with 89 percent utilizing this service. Overall, the underbanked use mobile banking for the same purposes as the general population, with only slightly lower rates for making bill payments (20 percent relative to 26 percent) and significantly higher rates for transferring money between their accounts (55 percent relative to 42 percent).

Although the underbanked are more likely than the general population to use mobile payments, the services that they use largely mirror those of the general

**Figure 8. Please choose the reason why you do not have a checking, savings, or money market account from the following list:**



Note: This was question 3 in the survey (see Appendix 1); number of respondents was 200.

population with one notable exception: the underbanked are substantially more likely to make bill payments using their mobile phones. Specifically, 62 percent of underbanked mobile payments users report paying bills, with their mobile phone in the past 12 months compared with 47 percent of the overall population of mobile phone users.

### Conclusion

The evolution of mobile technology has the potential to empower consumers and expand access to financial services for previously underserved populations. The prevalence of mobile phone access among minorities, low-income individuals, and younger generations creates the possibility of using mobile technology to expand financial inclusion to previously underserved populations.

The disproportionate use of mobile bill payment by the underbanked found in our survey is one example of how this technology can improve financial access for these groups. Mobile banking is poised for significant growth in adoption in the near future, with usage likely increasing to one in three mobile phone users by early 2013. Similarly, a significant fraction of mobile phone users appears to be interested in using phones to make mobile payments.

Consumers' perception that mobile banking and mobile payments are unsecure is currently one of the primary impediments to adoption. If consumers' perception of security issues changes—whether due to actual or perceived improvements—adoption rates may significantly increase.

## Appendix 1: Survey of Consumers' Financial Decisionmaking Using New Technologies—Questionnaire

Below is an exact reproduction of the survey instrument. The bracketed text are programming instructions that (1) indicate whether or not a question is single choice [SP] or multiple choice [MP] and (2) represent any skip pattern used to reach that question and which questions should be grouped together on a page. The respondents only saw the questions and response options; they did not see the program code.

### [DISPLAY]

The Federal Reserve Board is interested in learning more about how people manage their finances, shop, and make payments. We are especially interested in how people use mobile phones and other technology when making financial decisions.

To begin, we are going to ask a few questions about the types of financial products and services that you use.

### Banking Section

[SP]

1. Do you or does your spouse/partner currently have a checking, savings, or money market account?
  - a. Yes
  - b. No

[SP]

[IF Q1 = B]

2. Have you or your spouse/partner ever had a checking, savings, or money market account?
  - a. Yes
  - b. No

[SP]

[IF Q1 = B; shown on the same screen as Q2]

3. Please choose the **most important reason** why you don't have a checking, savings, or money market account from the following list:

- a. I don't write enough checks to make it worthwhile
- b. The minimum balance is too high
- c. I don't like dealing with banks
- d. The fees and service charges are too high
- e. No bank has convenient hours or locations
- f. No bank will give me an account g.
- g. Other (Please specify):[TXT]\_\_\_\_\_

[SP]

4. A payday loan (also called a paycheck advance or deposit advance) is a small, short-term loan that is intended to cover your expenses until your next payday. Firms that offer these loans generally charge fees for every \$100 borrowed (for example, \$15 or more). Have you or your spouse/partner ever used payday loans, paycheck advance, or deposit advance services?
- a. Yes
  - b. No

[NUMBER BOX, RANGE: 0-999, IF Q4= A]

5. How many times in the last 12 months did you or your spouse/partner use payday loan or payday advance services? In answering this question, please count a rollover of a payday loan as a new loan and also count using one payday loan to pay off another as separate loans.
- \_\_\_\_\_ time(s) in the past 12 months

[SP, IF Q4 = A; shown on the same screen as Q5]

6. What was the main reason for using a payday loan or payday advance services rather than a bank loan or credit card?
- a. The location of the payday lender was more convenient
  - b. The payday loan was much quicker to get than a bank loan or credit card
  - c. It was easier to get a payday loan than to qualify for a bank loan or credit card
  - d. It felt more comfortable to work with the payday lender than to use a bank
  - e. I didn't want the loan to show up on my credit report
  - f. I didn't think I would qualify for a bank loan or credit card
  - g. Other (Please specify):[TXT]\_\_\_\_\_

[DISPLAY]

A prepaid card is a card where funds are loaded or added to a card and then you access those funds with the card number or by swiping the card. It works like a debit card except that it is not connected to your bank account. A prepaid card is NOT a credit card.

There are four kinds of prepaid cards you may have seen before:

- 1) Gift cards are prepaid cards that you can only use at specific stores. Examples of these include department store cards and coffee shop cards.
- 2) General purpose prepaid cards are like gift cards except you can use them at many places. For example, a general purpose prepaid card can be used at grocery stores, clothing stores, gas stations, and so forth. These cards usually have a Visa or MasterCard logo on them.
- 3) Payroll cards are cards used by employers instead of a paycheck or direct deposit. These cards can be used to make purchases at many stores, and to make online payments and ATM withdrawals. They usually have a Visa or MasterCard logo on them.
- 4) Government issued prepaid cards are given to people who receive government benefits. Examples of these cards include Direct Express and Electronic Benefit Transfer (EBT) cards. These cards can be used to make purchases or payments, but may have restrictions on what you can purchase and where you can use them. In the rest of the survey, you can click on the text of these four kinds of prepaid cards (in blue) to see their definitions.

In the rest of the survey, you can click on the text of these four kinds of prepaid cards (in blue) to see their definitions.

**[PROGRAM INSTRUCTION]**

**DEFINITIONS. MAKE ALL INSTANCES FOR GIFT CARD, GENERAL PURPOSE PREPAID CARD, PAYROLL CARD, AND GOVERNMENT CARD IN THE SURVEY CLICKABLE. DISPLAY A CORRESPONDING DEFINITION. LET THE "CLICKABLE" TEXT AS A SIMPLE POPUP WINDOW THAT POPS UP IN A SMALLER SEPARATE WINDOW EVERY TIME R CLICK ON THE PHRASE.**

Gift card. Gift cards are prepaid cards that you can only use at specific stores. Examples of these include department store cards and coffee shop cards.

General purpose prepaid card. General purpose prepaid cards are like gift cards except you can use them at many places. For example, a general purpose prepaid card can be used at grocery stores, clothing stores, gas stations, and so forth. These cards usually have a Visa or MasterCard logo on them.

Payroll card. Payroll cards are cards used by employers instead of a paycheck or direct deposit. These cards can be used to make purchases at many stores, and to make online payments and ATM withdrawals. They usually have a Visa or MasterCard logo on them.

Government issued prepaid card. Government issued prepaid cards are given to people who receive government benefits. Examples of these cards include Direct Express and Electronic Benefit Transfer (EBT) cards. These cards can be used to make purchases or payments, but may have restrictions on what you can purchase and where you can use them.

[MP]

7. Do you have any of the following types of prepaid cards
- Gift card
  - General purpose prepaid card
  - Payroll card
  - Government card
  - None of the above **[Exclusive]**

[SP, IF Q7=A OR Q7=B OR Q7=C]

8. Some general purpose and merchant specific prepaid cards can be reloaded with extra dollar value by the card holder. Are any of your prepaid cards reloadable?
- Yes
  - No
  - Don't know

[SP, IF Q8 = A]

9. In the past 12 months, did you add money to reload any of your prepaid cards?
- Yes
  - No

[SP, IF Q9 = A]

10. Think about the prepaid card that you reload most often. When was the last time that you personally reloaded that prepaid card?
- In the past 7 days
  - In the past 30 days
  - In the past 90 days
  - In the past 12 months
  - More than 12 months ago
  - Never

[MP]

11. Which of the following financial products or services have you used in the past 12 months?
- Debit card or check card
  - Paper check
  - Major credit card (VISA, MasterCard, American Express, Discover)
  - Store-branded credit card good only at the store that issued the card
  - General purpose prepaid card

- f. Auto title loan
- g. Check cashing services
- h. Payday loans
- i. Layaway plan
- j. I use none of the products listed above **[Exclusive]**

**[SP, IF Q1 = A]**

12. **Telephone banking** is when you access your account by calling a phone number that your bank has provided. You interact with the system using either voice commands, your phone's numeric keypad, or speaking with a live customer service representative. It does not include accessing your bank using the internet or applications on your mobile phone.

Have you used telephone banking in the past 12 months, either with a land-line phone or your mobile phone?

- a. Yes
- b. No

**[MP, IF Q12 = A]**

13. Which of the following transactions have you done using telephone banking in the past 12 months?
- a. Checked account balances or transactions
  - b. Transferred money between accounts
  - c. Paid bills
  - d. Asked a customer service question
  - e. Deposited money
  - f. Applied for a credit card or loan
  - g. Other

**[DISPLAY]**

In this section we'll ask a few questions about your use of the internet. Right now we are just interested in your use of the internet on a computer (desktop, laptop, or tablet). Later on we will ask about use of the internet on mobile phones.

**[SP]**

14. Do you currently have regular access to the internet, either at home or outside your home (i.e. school, work, public library, etc)?
- a. Yes
  - b. No

**[SP, IF Q14 = A]**

15. Where do you use the internet the most often?

- a. At home
- b. At work
- c. At school
- d. At a library
- e. At someone else's home
- f. At an internet café or store with Wi-Fi
- g. Other

[SP, IF Q14 = A AND Q1 = A]

16. **Online banking** involves checking your account balance and recent transactions, transferring money, paying bills, or conducting other related transactions with your bank or credit card company using the internet.

Have you used online banking on a desktop, laptop or tablet computer in the past 12 months?

- a. Yes
- b. No

[MP, IF Q16 = A]

17. Which of the following transactions have you done using online banking on a desktop, laptop or tablet computer in the past 12 months?
- a. Checked account balances or transactions
  - b. Transferred money between accounts
  - c. Paid bills
  - d. Asked a customer service question
  - e. Deposited money
  - f. Applied for a credit card or loan
  - g. Managed investments (i.e. bought and sold stock or mutual funds)
  - h. Other

#### Screener Question on Mobile Phone Usage

[DISPLAY]

In this section we would like to ask you about your use of mobile phones (cell phones). You may be able to use your mobile phone to check bank account balances, transfer funds, pay bills, or carry out other financial transactions. Mobile phones are also being used to make payments to stores, for parking, or to another person. Mobile phones can help you shop by comparing prices or looking up product reviews while you are in the store.

[SP, PROMPT, TERMINATE IF SKIPPED]

18. Do you own or have regular access to a mobile phone (cell phone)?
- Yes **[MOBILE = "YES"]**
  - No **[MOBILE = "NO"]**

DOV: MOBILE

1: "YES"

2: "NO"

[SP]

**[MOBILE = "YES"]**

19. A smartphone is a mobile phone with features that may enable it to access the web, send e-mails, and interact with computers. Smartphones include the iPhone, BlackBerrys, as well as Android and Windows Mobile powered devices.
- Is your mobile phone a smart phone?
- Yes
  - No

[SP]

**[IF Q19 = A]**

20. Which type of smart phone do you have?
- Android
  - Blackberry
  - iPhone
  - Windows Mobile
  - Other
  - Don't know

[SP]

**[IF Q19 = A; shown on the same screen as Q20]**

21. When was the last time that you used the internet on your mobile phone?
- In the past 7 days
  - In the past 30 days
  - In the past 90 days
  - In the past 12 months
  - More than 12 months ago
  - Never

### Mobile Banking Users

[MOBILE = "YES"]

[DISPLAY]

**Mobile banking** uses a mobile phone to access your bank account, credit card account, or other financial account. This can be done either by accessing your bank's web page through the web browser on your mobile phone, via text messaging, or by using an application downloaded to your mobile phone.

[SP]

22. Have you used mobile banking in the past 12 months?
- Yes
  - No

[SP]

[IF Q22 = B]

23. Do you plan to use mobile banking in the next 12 months?
- Definitely will use
  - Probably will use
  - Probably will not use
  - Definitely will not use

[SP]

[IF Q23 = C OR Q23 = D]

24. Do you think you will ever use mobile banking?
- Definitely will use
  - Probably will use
  - Probably will not use
  - Definitely will not use

[MP]

[IF Q22 = A]

25. Using your mobile phone, have you done any of the following in the past 12 months?
- Downloaded your bank's mobile banking application on your mobile phone
  - Checked an account balance or checked recent transactions

- c. Made a bill payment using your bank's online banking website or banking application
- d. Received a text message alert from your bank
- e. Transferred money between two accounts
- f. Deposited a check to your account using your phone's camera
- g. Located the closest in-network ATM for your bank
- h. Managed your investments (i.e. bought and sold stock or mutual funds)
- i. Other banking-related activities (Please specify):[TXT]\_\_\_\_\_

[IF Q22 = A; NUMBER BOX; RANGE: 0-999; shown on the same screen as Q25]

26. In a typical month, how many times do you personally use mobile banking? If never please enter "0". \_\_\_\_\_ times

[SP]

[IF Q22 = A; shown on the same screen as Q25]

27. Overall, how satisfied are you with your mobile banking experiences?
- a. Very satisfied
  - b. Somewhat satisfied
  - c. Somewhat dissatisfied
  - d. Very dissatisfied

[MP; ONLY TWO CHOICES PERMITTED, IF MORE THAN TWO, PROMPT "PLEASE SELECT ONLY TWO CHOICES."]

[IF Q27 = C OR Q27 = D]

28. What are the top two reasons you are dissatisfied with your mobile banking experiences?
- a. I am concerned about my personal information being disclosed or have had personal information disclosed as a result of mobile banking
  - b. Applications and/or websites for mobile banking are too complicated to use
  - c. I have had problems getting the websites or applications to work properly
  - d. Banking on my mobile phone takes too long
  - e. It is too difficult to see on my mobile phone's screen
  - f. The transactions I want to execute are not available
  - g. Other (Please specify):[TXT]\_\_\_\_\_

### Mobile Payments Users

[MOBILE = "YES"]

[DISPLAY]

**Mobile payments** are purchases, bill payments, charitable donations, payments to another person, or any other payments made using a mobile phone. You can do this either by accessing a web page through the web browser on your mobile device, by sending a text message (SMS), or by using a downloadable application on your mobile device. The amount of the payment may be applied to your phone bill (for example Red Cross text message donation), charged to your credit card, or withdrawn directly from your bank account.

[SP]

29. Have you made a mobile payment in the past 12 months?
- Yes
  - No

[MP]

[IF Q29 = A]

30. Using your mobile phone, have you done any of the following in the past 12 months?
- Transferred money directly to another person's bank, credit card or PayPal account (i.e. friend, relative)
  - Received money from another person using my mobile phone
  - Waved or tapped my mobile phone at the cash register to pay for a purchase
  - Paid bills online (excluding payments made directly from your bank website or application)
  - Made a charitable donation by text message
  - Transferred money to friends or family in another country
  - Used my mobile phone as a "virtual wallet" to replace the cards I previously carried in my wallet
  - Made online purchases
  - None of the above **[Exclusive]**

[MP]

[IF Q30 = A to H]

31. Do you make your mobile payments using a credit card number, your bank account, adding the charge to your phone bill, or through a service such as Paypal, Google Wallet, or iTunes, which indirectly charges your credit card or bank account? (Select all that apply)

- a. Credit card, debit card or prepaid card number
- b. Bank account
- c. Charged to your phone bill
- d. Paypal, Google Wallet, iTunes, etc.
- e. Other (Please specify):[TXT] \_\_\_\_\_

[MP]

**[IF Q29 = A]**

32. Have you used any of the following methods to make or receive mobile payments in the past 12 months?
- a. Used a text message to make or receive a mobile payment
  - b. Waved or tapped my mobile phone at the cash register or other payment sensor
  - c. Scanned a barcode using your mobile phone to make a mobile payment
  - d. Used your mobile phone's web browser to make or receive a mobile payment
  - e. Used a downloadable app to make or receive a mobile payment
  - f. None of the above **[Exclusive]**

**[IF Q29 = A; NUMBER BOX; RANGE: 0-99; shown on the same screen as Q32]**

33. In a typical month, how many times do you use your mobile phone to make payments? If never please enter "0". \_\_\_\_\_times

[SP]

**[IF Q29 = A; shown on the same screen as Q32]**

34. Overall, how satisfied are you with your mobile payment experiences?
- a. Very satisfied
  - b. Somewhat satisfied
  - c. Somewhat dissatisfied
  - d. Very dissatisfied

[MP, ONLY TWO CHOICES PERMITTED, IF MORE THAN TWO, PROMPT "PLEASE SELECT ONLY TWO CHOICES."]

**[IF Q34 = C OR Q34 = D]**

35. What are the top two reasons you are dissatisfied with your mobile payment experiences? (Select only two choices)
- a. I am concerned about my personal information being disclosed or have had personal information disclosed as a result of making mobile payments

- b. I find that applications and/or websites for mobile payments are too complicated to use
- c. I have had problems getting the websites or applications to work properly
- d. It is too difficult to see on my mobile phone's screen
- e. Making mobile payments takes too long
- f. Making mobile payments is much more complicated than using another payment method
- g. Merchants don't generally accept mobile payments
- h. The transactions I want to execute are not available
- i. Other (Please specify):[TXT]\_\_\_\_\_

### Non-Mobile Banking Users

[IF Q22 = B]

[DISPLAY]

We would like to ask you about some of your reasons for not using mobile banking

[MP]

[IF Q22 = B]

36. You indicated that you do not currently use mobile banking. What are the main reasons why you have decided not to use mobile banking?
- a. I'm concerned about the security of mobile banking
  - b. My banking needs are being met without mobile banking
  - c. The cost of data access on my wireless plan is too high
  - d. It is too difficult to see on my mobile phone's screen
  - e. It is not offered by my bank or credit union
  - f. My bank charges a fee for using mobile banking
  - g. I don't trust the technology to properly process my banking transactions
  - h. I don't have a banking account with which to use mobile banking
  - i. It's difficult or time consuming to set up mobile banking
  - j. Other (Please specify):[TXT]\_\_\_\_\_

[SP]

[IF Q36 = A]

37. You mentioned that security was one of your top concerns with mobile banking. What security aspects are you most concerned with?

- a. Hackers gaining access to my phone remotely
- b. Someone intercepting my calls or data
- c. Losing my phone or having my phone stolen
- d. Malware or viruses being installed on my phone
- e. Other (Please specify):[TXT]\_\_\_\_\_

[MP]

**[IF Q22 = B]**

38. Assuming that any concerns you have about mobile banking were addressed, which of the following activities would you be interested in doing with your mobile phone?
- a. Download your bank's mobile banking application on your mobile phone
  - b. Check an account balance or check recent transactions
  - c. Make a bill payment using your bank's online banking website or banking application
  - d. Receive text message alerts from your bank
  - e. Transfer money between two accounts
  - f. Other banking-related activities (Please specify):[TXT]\_\_\_\_\_

### Non-Mobile Payments Users

**[IF Q29 = B]**

**[DISPLAY;** shown on the same page as 39]

We would like to ask you about some of your reasons for not using mobile payments

[MP]

**[IF Q29 = B]**

39. You indicated that you do not use mobile payments. What are the main reasons why you have decided not to use mobile payments?
- a. I'm concerned about the security of mobile payments
  - b. It's easier to pay with another method like cash or a credit card
  - c. I don't see any benefit from using mobile payments
  - d. I don't know of any stores that let you pay with your mobile phone
  - e. I don't have the necessary feature on my phone
  - f. The cost of data access on my wireless plan is too high
  - g. It is not offered by my bank or credit union

- h. My bank charges a fee for using mobile payments
- i. I don't trust the technology to properly process my payments
- j. It's difficult or time consuming to set up mobile payments
- k. Other (Please specify):[TXT]\_\_\_\_\_

[SP]

**[IF Q39 = A]**

40. You mentioned that security was one of your top concerns with mobile payments. What security aspect are you most concerned with?
- a. Hackers gaining access to my phone remotely
  - b. Someone intercepting my payment information or other data
  - c. Losing my phone or having my phone stolen
  - d. Malware or viruses being installed on my phone
  - e. Other (Please specify):[TXT]\_\_\_\_\_

[MP]

**[IF Q29 = B]**

41. Assuming that the reason(s) why you do not currently use mobile payments was addressed, which of the following activities would you be interested in doing with your mobile phone?
- a. Making payments directly to another person (i.e. friend, relative)
  - b. Waving or tapping my mobile phone at the cash register to pay for a purchase
  - c. Paying bills online
  - d. Transferring money to friends or family in another country
  - e. Using your mobile phone as a "virtual wallet" to replace all the cards you currently carry in your wallet
  - f. Buying goods or services online
  - g. Receiving/using coupons on your phone
  - h. Receiving specials and discount offers based on your location
  - i. Other payment-related activities (Please specify):[TXT]\_\_\_\_\_

[SP]

**[IF Q1 = B]**

**Mobile Financial Services Security Questions**

[MOBILE = "YES" FOR QUESTIONS 42 THROUGH 47]

[DISPLAY, SHOW IT ON THE SAME SCREEN WITH Q42 TO Q45]

Please rate the level of security of each of the following four methods for mobile banking from Very Safe to Very Unsafe.

[SP]

42. SMS (text messaging)

- a. Very safe
- b. Somewhat safe
- c. Somewhat unsafe
- d. Very unsafe
- e. Don't know

[SP]

43. Mobile browser similar to the way you access the internet on your PC

- a. Very safe
- b. Somewhat safe
- c. Somewhat unsafe
- d. Very unsafe
- e. Don't know

[SP]

44. Application downloaded from your phone's mobile app store

- a. Very safe
- b. Somewhat safe
- c. Somewhat unsafe
- d. Very unsafe
- e. Don't know

[SP]

45. How would you currently rate the overall security of mobile banking for protecting your personal information?

- a. Very safe
- b. Somewhat safe
- c. Somewhat unsafe
- d. Very unsafe

e. Don't know

[MP]

46. Would you like to use your mobile phone for any of the following purposes, assuming they were made available to you?
- Buy things at the point of sale
  - Track your finances on a daily basis
  - Organize and track gift cards, loyalty and reward points
  - Compare prices when shopping
  - As a ticket for buses, trains, or subways
  - As a key to enter your house
  - Purchase tickets to events
  - As a membership card (such as museums, gym, etc.)
  - To receive and manage discount offers and coupons
  - To receive offers and promotions based on where you are (i.e. You walk into a store and a coupon appears on your mobile phone for a product sold there)
  - As a form of photo identification

[SP]

47. Banks can offer a service whereby checks to be deposited are photographed using your camera phone and the image is sent over the mobile Internet during a mobile banking session so that the bank can deposit the funds into your account without you having to present the physical check. The bank then sends a notification acknowledging receipt of the deposit.

If your bank offered this service, how likely would you be to use it?

- I already use it
- Very likely
- Somewhat likely
- Somewhat unlikely
- Very unlikely

### Shopping Behavior Questions

[ASKED OF EVERYONE]

[DISPLAY]

In this section we would like to ask you about your shopping habits.

[SP]

**[IF Q14 = A]**

48. Before going to a retail store to make a large purchase, do you generally compare prices online?
- a. Yes
  - b. No

[SP]

**[IF Q14 = A; shown on the same screen as Q48]**

49. Before going to a retail store to make a large purchase, do you generally look at product reviews online?
- a. Yes
  - b. No

[SP]

**[IF MOBILE = "YES"]**

50. Online shopping is when you go to a merchant's website through your web browser or an application and make a purchase. Have you ever used your mobile phone for online shopping?
- a. Yes
  - b. No

[SP]

**[IF MOBILE = "YES"; shown on the same screen as Q50]**

51. Have you ever used your mobile phone to comparison shop over the internet while at a retail store?
- a. Yes
  - b. No

[SP]

**[IF MOBILE = "YES"; shown on the same screen as Q50]**

52. Have you ever used a barcode scanning application on your mobile phone while shopping at a retail store to find the best price for an item?
- a. Yes
  - b. No

[SP]

**[IF Q51 = A OR Q52 = A]**

53. Has using your mobile phone to compare prices while you were shopping at a retail store ever changed where you made your purchase?

- a. Yes
- b. No

[SP]

**[IF MOBILE = "YES"]**

54. Have you ever used your mobile phone to browse product reviews while shopping at a retail store?

- a. Yes
- b. No

[SP]

**[IF Q54 = A]**

55. Has reading product reviews on your mobile phone while shopping at a retail store ever changed which item you ended up purchasing?

- a. Yes
- b. No

[SP]

**[IF Q22 = A]**

56. In the past 12 months, have you used your mobile phone to check your account balance or available credit before making a large purchase?

- a. Yes
- b. No

[SP]

**[IF Q56 = A]**

57. Thinking of the most recent time that you used your mobile phone to check your account balance or available credit before making a large purchase did you decide not to buy that particular item because of the amount of money left in your account or the amount of your available credit?

- a. Yes
- b. No

[SP]

**[ASKED OF EVERYONE]**

58. Have you signed up to receive coupons or special offers by e-mail from retail stores in the past 12 months?

- a. Yes
- b. No

[SP]

**[IF Q58 = A]**

59. Have you made a purchase as a result of receiving one of these coupons or special offers?

- a. Yes
- b. No

[SP]

**[ASKED OF EVERYONE]**

60. Have you ever signed up to receive coupons/offers from a website such as Groupon or Living Social?

- a. Yes
- b. No

[SP]

**[IF Q60 = A]**

61. Have you ever used a coupon from a website such as Groupon or Living Social?

- a. Yes
- b. No

**Payments Choice**

**[MOBILE = "YES"]**

**[DISPLAY]**

In this section we would like to ask about your thoughts on some of the new mobile financial service technologies.

[SP]

**[MOBILE = "YES"]**

62. New **mobile** "contactless" payments are becoming available from some banks, credit card companies, and transit operators. These let consumers "tap" or wave their mobile phone at a terminal instead of swiping a card.

If you were offered the option of using this service, how likely would you be to use it?

- a. I already use it
- b. Very likely
- c. Somewhat likely
- d. Somewhat unlikely
- e. Very unlikely

[SP]

[MOBILE = "YES"; shown on the same screen as Q62]

63. How likely do you think it is that mobile contactless payments will become a major form of payment in the next five years?
- a. Very likely
  - b. Somewhat likely
  - c. Somewhat unlikely
  - d. Very unlikely
  - e. Don't know

#### Financial Management (Saving, Budgeting) Questions

[ASKED OF EVERYONE]

[DISPLAY, SHOW IT ON THE SAME SCREEN WITH Q64 TO Q67]

In order to help us to understand your role in the financial activities of your household, please rank how much responsibility you have for the following four financial tasks

[SP]

64. Maintaining the household budget and managing household income
- a. None or almost none
  - b. Some
  - c. Shared equally with other household members
  - d. Most
  - e. All or almost all

[SP]

65. Paying monthly bills (rent or mortgage, utilities, cell phone, etc.)
- a. None or almost none
  - b. Some
  - c. Shared equally with other household members

- d. Most
- e. All or almost all

[SP]

66. Shopping for household goods and groceries
- a. None or almost none
  - b. Some
  - c. Shared equally with other household members
  - d. Most
  - e. All or almost all

[SP]

67. Making decisions about saving and investments (whether to save, how much to save, where to invest)
- a. None or almost none
  - b. Some
  - c. Shared equally with other household members
  - d. Most
  - e. All or almost all

[SP]

68. Do you or anyone in your household use a program or website to track your household finances (for example, Quicken, Mint.com, Excel, or a website provided by your bank)?
- a. Yes
  - b. No

[SP, IF Q68= A]

69. How long have you been using this program or website to manage your household finances?
- a. Less than a year
  - b. One to two years
  - c. Three to five years
  - d. More than five years

[IF Q68= A; NUMBER BOX; RANGE: 0-999; shown on the same screen as Q69]

70. In a typical month, how often do you or another household member use this program or website? (If never please enter "0") \_\_\_\_\_ times

[SP, IF MOBILE= "YES"]

71. Do you use your mobile phone to track purchases and expenses?
- Yes
  - No

**[MP, IF Q71= A]**

72. What method(s) do you use to track purchases and expenses on your mobile phone?
- A mobile application for expense tracking
  - A spreadsheet
  - Online (using the web browser to access a website)
  - Send text messages
  - Take notes in a notepad or word processor

**[IF Q71= A; NUMBER BOX; RANGE: 0-999; shown on the same screen as Q72]**

73. In a typical month, how often do you use your mobile phone to track purchases and expenses? (If never please enter "0") \_\_\_\_\_times

**[MP, IF Q25= D]**

74. You previously mentioned that you receive text alerts from your bank. What kind of text alerts do you receive?
- Low-balance alerts
  - Payment due alerts
  - Saving reminders
  - Fraud alerts
  - Other (Please specify): **[TXT]** \_\_\_\_\_

**[MP, IF Q74= A]**

75. Thinking of the most recent low-balance alert you received by text message, which of the following actions did you take after receiving the alert?
- Transferred money into the account with the low-balance
  - Deposited money into the account with the low-balance
  - Reduced my spending
  - None of the above **[Exclusive]**

**[SP, IF Q74= B]**

76. Has receiving payment due alerts improved your ability to pay your bills on time?
- Yes, by a lot
  - Yes, by a little

c. No

### Financial Literacy Questions

[ASKED OF EVERYONE]

[SP]

77. Imagine that the interest rate on your savings account was 1% per year and inflation was 2% per year. After 1 year, how much would you be able to buy with the money in this account?
- More than today
  - Exactly the same
  - Less than today

[SP; shown on the same screen as Q77]

78. Considering a long time period (for example, 10 or 20 years), which asset normally gives the highest return?
- Savings accounts
  - U.S. Government bonds
  - Stocks

[SP; shown on the same screen as Q77]

79. If an investor who only owns two stocks right now decides to instead spread their money among many different assets (i.e. more stocks, add bonds, add real estate), their risk of losing money on their entire portfolio will:
- Increase
  - Decrease
  - Stay the same

[SP]

80. If you were to invest \$1000 in a stock mutual fund for a year, it would be possible to have less than \$1000 when you withdraw your money.
- True
  - False

[SP; shown on the same screen as Q80]

81. Suppose you owe \$1,000 on a loan and the interest rate you are charged is 10% per year compounded annually. If you didn't make any payments on this loan, at this interest rate, how many years would it take for the amount you owe to double?
- Less than 2 years

- b. Between 2 and 5 years
- c. 5 to 9 years
- d. 10 years or more

[MP]

82. Imagine that your car breaks down and requires \$400 worth of repairs in order to drive again. **Based on your current financial situation**, how would you pay for this expense? If you would use more than one method to cover this expense please select all that apply.

- a. Put it on my credit card
- b. With the money currently in my checking account
- c. By taking money out of my savings
- d. Using money from a bank loan, line of credit, or overdraft
- e. By borrowing from a friend or family member
- f. Using a payday loan or deposit advance
- g. By pawning something
- h. Other (Please specify): [TXT] \_\_\_\_\_

#### Risk Aversion Questions

[ASKED OF EVERYONE]

[SP]

83. Which of the following statements comes closest to describing the amount of financial risk that you are willing to take when you save or make investments?

- a. Take substantial financial risks expecting to earn substantial returns
- b. Take above average financial risks expecting to earn above average returns
- c. Take average financial risks expecting to earn average returns
- d. Not willing to take any financial risks

[SP]

84. Suppose that you are the only income earner in the family, and you have a good job guaranteed to give you your current income every year for life. You are given the opportunity to take a new and equally good job, with a 50-50 chance that it will double your income and a 50-50 chance that it will cut your income by one-third (33 percent). Would you take the new job?

- a. Yes
- b. No

[SP]

**[IF Q84 = A]**

85. Now suppose that the chances were 50–50 that it would double your income and 50–50 that it would cut your income by half (50 percent). Would you still take the new job?

- a. Yes
- b. No

[SP]

**[IF Q84 = B]**

86. Now suppose that the chances were 50–50 that it would double your income and 50–50 that it would cut your income by one-fifth (20 percent). Would you now take the new job?

- a. Yes
- b. No

## Appendix 2: Consumer Responses to Survey Questionnaire

**Table B.1. Do you or does your spouse/partner currently have a checking, savings, or money market account?**

Percent, except as noted

Q1	
Yes	88.7
No	10.8
Refused to answer	0.5
<b>Number of respondents</b>	<b>2,290</b>

**Table B.4. Have you or your spouse/partner ever used payday loans, paycheck advance, or deposit advance services?**

Percent, except as noted

Q4	
Yes	11.2
No	88.1
Refused to answer	0.8
<b>Number of respondents</b>	<b>2,290</b>

**Table B.2. Have you or your spouse/partner ever had a checking, savings, or money market account?**

Percent, except as noted

Q2	
Yes	36.9
No	58.9
Refused to answer	4.2
<b>Number of respondents</b>	<b>200</b>

**Table B.5. How many times in the last 12 months did you or your spouse/partner use payday loan or payday advance services? In answering this question, please count a rollover of a payday loan as a new loan and also count using one payday loan to pay off another as separate loans.**

Percent, except as noted

Q5	
0	44.9
1	13.8
2	11.6
3	6.3
4	3.9
5	5.3
6	3.1
7	0.3
8	0.9
9	0.1
10	2.6
12	2.1
16	0.5
20	0.5
24	0.3
40	0.6
Refused to answer	3.1
<b>Number of respondents</b>	<b>223</b>

**Table B.3. Please choose the most important reason why you don't have a checking, savings, or money market account from the following list.**

Percent, except as noted

Q3	
I don't write enough checks to make it worthwhile	23.5
The minimum balance is too high	2.2
I don't like dealing with banks	24.2
The fees and service charges are too high	13.3
No bank has convenient hours or locations	0.6
No bank will give me an account	10.2
Other	17.8
Refused to answer	8.1
<b>Number of respondents</b>	<b>200</b>

**Table B.6. What was the main reason for using a payday loan or payday advance service rather than a bank loan or credit card?**

Percent, except as noted

Q6	
The location of the payday lender was more convenient	3.6
The payday loan was much quicker to get than a bank loan or credit card	17.7
It was easier to get a payday loan than to qualify for a bank loan or credit card	24.9
It felt more comfortable to work with the payday lender than to use a bank	1.2
I didn't want the loan to show up on my credit report	2.1
I didn't think I would qualify for a bank loan or credit card	29.2
Other	8
Refused to answer	13.4
Number of respondents	223

**Table B.7. Do you have any of the following types of prepaid cards?**

Percent, except as noted

Q7	
Gift card	48
General purpose prepaid card	14.5
Payroll card	1.7
Government card	4.8
None of the above	45.4
Refused to answer	0.4
Number of respondents	2,290

**Table B.8. Some general purpose and merchant specific prepaid cards can be reloaded with extra dollar value by the cardholder. Are any of your prepaid cards reloadable?**

Percent, except as noted

Q8	
Yes	44.7
No	30.4
Don't know	24.5
Refused to answer	0.4
Number of respondents	1,228

**Table B.9. In the past 12 months, did you add money to reload any of your prepaid cards?**

Percent, except as noted

Q9	
Yes	40.3
No	59.7
Number of respondents	499

**Table B.10. Think about the prepaid card that you reload most often. When was the last time that you personally reloaded that prepaid card?**

Percent, except as noted

Q10	
In the past 7 days	21.2
In the past 30 days	41.1
In the past 90 days	20
In the past 12 months	17.1
More than 12 months ago	0.6
Never	0.1
Number of respondents	207

**Table B.11. Which of the following financial products or services have you used in the past 12 months?**

Percent, except as noted

Q11	
Debit card or check	69
Paper check	66.7
Major credit card	60.2
Store-branded credit card good only at the store that issued the card	30.2
General purpose prepaid card	18.6
Auto title loan	3.5
Check cashing service	4.1
Payday loan	3.3
Layaway plan	3.8
None of the above	7.2
Refused to answer	0.6
Number of respondents	2,290

**Table B.12. Have you used telephone banking in the past 12 months, either with a landline phone or your mobile phone?**

Percent, except as noted

Q12	
Yes	33.3
No	66.3
Refused to answer	0.4
Number of respondents	2,079

**Table B.13. Which of the following transactions have you performed using telephone banking in the past 12 months?**

Percent, except as noted

Q13	
Checked account balances or transactions	78.1
Transferred money between accounts	31.3
Paid bills	29.8
Asked a customer service question	44
Deposited money	4.8
Applied for a credit card or loan	2.4
Other	2.7
Refused to answer	0.3
Number of respondents	653

**Table B.14. Do you currently have regular access to the Internet, either at home or outside your home (i.e., school, work, public library)?**

Percent, except as noted

Q14	
Yes	95.4
No	4.3
Refused to answer	0.4
Number of respondents	2,290

**Table B.15. Where do you use the Internet the most often?**

Percent, except as noted

Q15	
At home	80.8
At work	14.8
At school	0.8
At a library	1.7
At someone else's home	1
At an Internet café or store with Wi-Fi	0.3
Other	0.3
Refused to answer	0.2
Number of respondents	2,189

**Table B.16. Have you used online banking on a desktop, laptop, or tablet computer in the past 12 months?**

Percent, except as noted

Q16	
Yes	67.7
No	31.9
Refused to answer	0.5
Number of respondents	2,011

**Table B.17. Which of the following transactions have you done using online banking on a desktop, laptop, or tablet computer in the past 12 months?**

Percent, except as noted

Q17	
Checked account balances or transactions	95.8
Transferred money between accounts	67.6
Paid bills	73.1
Asked a customer service question	11.8
Deposited money	11.9
Applied for a credit card or loan	8
Managed investments (i.e., bought and sold stock or mutual funds)	8.8
Other	0.8
Refused to answer	0.4
Number of respondents	1,358

**Table B.18. Do you own or have regular access to a mobile phone (cell phone)?**

Percent, except as noted

Q18	
Yes	87.1
No	12.9
Number of respondents	2,290

**Table B.19. Is your mobile phone a smartphone?**

Percent, except as noted

Q19	
Yes	43.9
No	55.9
Refused to answer	0.2
Number of respondents	2,002

**Table B.20. Which type of smartphone do you have?**

Percent, except as noted

Q20	
Android	43.4
BlackBerry	13.1
iPhone	30.1
Windows Mobile	1.2
Other	7.7
Don't know	3.9
Refused to answer	0.5
Number of respondents	836

**Table B.21. When was the last time that you used the Internet on your mobile phone?**

Percent, except as noted

Q21	
In the past 7 days	83.6
In the past 30 days	6.5
In the past 90 days	2.4
In the past 12 months	1.6
More than 12 months ago	0.3
Never	6.5
Refused to answer	0.1
Number of respondents	836

**Table B.22. Have you used mobile banking in the past 12 months?**

Percent, except as noted

Q22	
Yes	20.9
No	78.9
Refused to answer	0.2
Number of respondents	2,002

**Table B.23. Do you plan to use mobile banking in the next 12 months?**

Percent, except as noted Percent, except as noted

Q23	
Definitely will use	0.8
Probably will use	10.4
Probably will not use	39.6
Definitely will not use	48.6
Refused to answer	0.6
Number of respondents	1,626

**Table B.24. Do you think you will ever use mobile banking?**

Percent, except as noted

Q24	
Definitely will use	0.6
Probably will use	16.4
Probably will not use	45.4
Definitely will not use	36.9
Refused to answer	0.8
Number of respondents	1,449

**Table B.25. Using your mobile phone, have you done any of the following in the past 12 months?**

Percent, except as noted

Q25	
Downloaded your bank's mobile banking application on your mobile phone	48.1
Checked an account balance or checked recent transactions	90.1
Made a bill payment using your bank's online banking website or banking application	25.7
Received a text message alert from your bank	33.4
Transferred money between two accounts	41.7
Deposited a check to your account using your phone's camera	10.6
Located the closest in-network ATM for your bank	20.7
Managed your investments (i.e., bought and sold stock or mutual funds)	2.2
Other banking-related activities	1
Refused to answer	3
Number of respondents	372

**Table B.26. In a typical month, how many times do you personally use mobile banking?**

Percent, except as noted

Q26	
0	6
1	11.7
2	12.6
3	10.7
4	8.8
5	9.7
6	3.6
7	2.1
8	2.4
9	0.5
10	9.5
12	0.6
15	4.3
16	0.8
20	9.5
25	0.8
30	3.1
50	0.3
60	0.6
Refused to answer	2.4
Number of respondents	372

**Table B.27. Overall, how satisfied are you with your mobile banking experiences?**

Percent, except as noted

Q27	
Very satisfied	61.7
Somewhat satisfied	32.3
Somewhat dissatisfied	2.1
Very dissatisfied	1.1
Refused to answer	2.9
Number of respondents	372

**Table B.28. What are the top two reasons you are dissatisfied with your mobile banking experience?**

Frequency, except as noted

Q28	
I am concerned about my personal information being disclosed	5
I have had problems getting the websites or applications to work properly	4
Banking on my mobile phone takes too long	6
It is too difficult to see on my mobile phone's screen	3
The transactions I want to execute are not available	3
Other	7
<b>Number of respondents</b>	<b>14</b>

**Table B.31. Do you make your mobile payments using a credit card number, your bank account, adding the charge to your phone bill, or through a service such as Paypal, Google Wallet, or iTunes, that indirectly charges your credit card or bank account?**

Percent, except as noted

Q31	
Credit card, debit card, or prepaid card	66.4
Bank account	45.4
Charged to your phone bill	8.4
Paypal, Google Wallet, iTunes, etc.	21.9
Other	3.9
<b>Number of respondents</b>	<b>161</b>

**Table B.29. Have you made a mobile payment in the past 12 months?**

Percent, except as noted

Q29	
Yes	12.3
No	87.3
Refused to answer	0.4
<b>Number of respondents</b>	<b>2,002</b>

**Table B.32. Have you used any of the following methods to make or receive mobile payments in the past 12 months?**

Percent, except as noted

Q32	
Used a text message to make or receive a mobile payment	16.2
Waved or tapped my mobile phone at the cash register or other payment sensor	1.3
Scanned a barcode using your mobile phone to make a mobile payment	1
Used your mobile phone's web browser to make or receive a mobile payment	23
Used a downloadable app to make or receive a mobile payment	21
None of the above	45
Refused to answer	5.4
<b>Number of respondents</b>	<b>213</b>

**Table B.30. Using your mobile phone, have you done any of the following in the past 12 months?**

Percent, except as noted

Q30	
Transferred money directly to another person's bank, credit card, or paypal account	20.5
Received money from another person using my mobile phone	7.9
Waved or tapped my mobile phone at the cash register to pay for a purchase	2.4
Paid bills online (excluding payments made directly from your bank website or application)	47.1
Made a charitable donation via text message	5.1
Transferred money to friends or family in another country	0.2
Used my mobile phone as a "virtual wallet" to replace the cards I previously carried in my wallet	0.2
Made online purchases	36
None of the above	23
Refused to answer	0.4
<b>Number of respondents</b>	<b>213</b>

**Table B.33. In a typical month, how many times do you use your mobile phone to make payments?**

Percent, except as noted

Q33	
0	25
1	34.4
2	12.7
3	6.6
4	4.8
5	4.4
6	1.9
7	0.1
8	0.3
9	1.3
10	1.5
12	0.1
14	0.2
15	0.4
24	0.6
Refused to answer	5.7
<b>Number of respondents</b>	<b>213</b>

**Table B.34. Overall, how satisfied are you with your mobile payment experiences?**

Percent, except as noted

Q34	
Very satisfied	55.2
Somewhat satisfied	32.6
Somewhat dissatisfied	1.5
Very dissatisfied	3.3
Refused to answer	7.4
<b>Number of respondents</b>	<b>213</b>

**Table B.37. You mentioned that security was one of your top concerns with mobile banking. What security aspects are you most concerned with?**

Percent, except as noted

Q37	
Hackers gaining access to my phone remotely	54.3
Someone intercepting my calls or data	18.1
Losing my phone or having my phone stolen	19.3
Malware or viruses being installed on my phone	4.8
Other	3.3
Refused to answer	0.2
<b>Number of respondents</b>	<b>798</b>

**Table B.35. What are the top two reasons you are dissatisfied with your mobile payment experiences?**

Frequency, except as noted

Q35	
I am concerned about my personal information being disclosed or have had personal information disclosed	10
I find that applications and/or websites for mobile payments are too complicated to use	2
I have had problems getting the websites or applications to work properly	4
Making mobile payments takes too long	1
Making mobile payments is much more complicated than using another payment method	6
It is too difficult to see on my mobile phone's screen	2
Merchants don't generally accept mobile payments	2
Other	1
<b>Number of respondents</b>	<b>14</b>

**Table B.38. Assuming that any concerns you have about mobile banking were addressed, which of the following activities would you be interested in performing with your mobile phone?**

Percent, except as noted

Q38	
Download your bank's mobile banking application on your mobile phone	16.6
Check an account balance or check recent transactions	55.4
Make a bill payment using your bank's online banking website or banking application	23.7
Receive text message alerts from your bank	30.2
Transfer money between two accounts	24.5
Other banking-related activities	9
Refused to answer	12.6
<b>Number of respondents</b>	<b>1,626</b>

**Table B.36. You indicated that you do not use mobile banking. What are the main reasons why you have decided not to use mobile banking?**

Percent, except as noted

Q36	
I am concerned about the security of mobile banking	48
My banking needs are being met without mobile banking	57.5
The cost of data access on my wireless plan is too high	18.3
It is too difficult to see on my mobile phone's screen	16.6
It is not offered by my bank or credit union	2.7
My bank charges a fee for using mobile banking	2.2
I don't trust the technology to properly process my banking transactions	21.8
I don't have a banking account with which to use mobile banking	8.8
It is difficult or time consuming to set up mobile banking	9.5
Other	12.6
Refused to answer	0.6
<b>Number of respondents</b>	<b>1626</b>

**Table B.39. You indicated that you do not use mobile payments. What are the main reasons you have decided not to use mobile payments?**

Percent, except as noted

Q39	
I am concerned about the security of mobile payments	41.5
It is easier to pay with another method like cash or a credit card	36
I don't see any benefit from using mobile payments	36.7
I don't know of any stores that let you pay with your mobile phone	9
I don't have the necessary feature on my phone	30.8
The cost of data access on my wireless plan is too high	15.3
It is not offered by my bank or credit union	4.3
My bank charges a fee for using mobile payments	1.9
I don't trust the technology to properly process my payments	19.7
It is difficult or time consuming to set up mobile payments	9.1
Other	12.4
Refused to answer	1.7
<b>Number of respondents</b>	<b>1,780</b>

**Table B.40. You mentioned that security was one of your top concerns with mobile payments. What security aspect are you most concerned with?**

Percent, except as noted

Q40	
Hackers gaining access to my phone remotely	46.6
Someone intercepting my payment information or other data	32.8
Losing my phone or having my phone stolen	16.6
Malware or viruses being installed on my phone	2.7
Other	1.7
Refused to answer	0.6
<b>Number of respondents</b>	<b>745</b>

**Table B.43. Please rate the security of mobile browsers similar to the way you access the Internet on your PC.**

Percent, except as noted

Q43	
Very safe	5.6
Somewhat safe	36
Somewhat unsafe	18.8
Very unsafe	7.6
Don't know	30.2
Refused to answer	2
<b>Number of respondents</b>	<b>2,002</b>

**Table B.41. Assuming that the reason(s) you do not currently use mobile payments was addressed, which of the following activities would you be interested in performing with your mobile phone?**

Percent, except as noted

Q41	
Making payments directly to another person	17.1
Waving or tapping my mobile phone at the cash register to pay for a purchase	17.2
Paying bills online	34.4
Transferring money to friends or family in another country	7
Using your mobile phone as a "virtual wallet" to replace all the cards you currently carry in your wallet	16.6
Buying goods or services online	21.9
Receiving/using coupons on your phone	27.7
Receiving specials and discount offers based on your location	21.6
Other payment-related activities	12
Refused to answer	15.2
<b>Number of respondents</b>	<b>1,780</b>

**Table B.44. Please rate the security of an application downloaded from your phone's mobile app store.**

Percent, except as noted

Q44	
Very safe	7.4
Somewhat safe	32.9
Somewhat unsafe	15.1
Very unsafe	6.8
Don't know	36.1
Refused to answer	1.8
<b>Number of respondents</b>	<b>2,002</b>

**Table B.42. Please rate the security of SMS (text messaging).**

Percent, except as noted

Q42	
Very safe	8.3
Somewhat safe	30.1
Somewhat unsafe	16.4
Very unsafe	10.8
Don't know	33.1
Refused to answer	1.2
<b>Number of respondents</b>	<b>2,002</b>

**Table B.45. How would you currently rate the overall security of mobile banking for protection?**

Percent, except as noted

Q45	
Very safe	5.1
Somewhat safe	27.8
Somewhat unsafe	20.7
Very unsafe	11.2
Don't know	33.9
Refused to answer	1.4
<b>Number of respondents</b>	<b>2,002</b>

**Table B.46. Would you like to use your mobile phone for any of the following purposes, assuming they were made available to you?**

Percent, except as noted

Q46	
Buy things at the point of sale	26.2
Track your finances on a daily basis	31.1
Organize and track gift cards, loyalty and reward points	21.4
Compare prices when shopping	47.9
As a ticket for buses, trains, or subways	18.7
As a key to enter your house	18.4
Purchase tickets to events	22.9
As a membership card (e.g., museums, gym, etc.)	24.2
To receive and manage discount offers and coupons	30.5
To receive offers and promotions based on where you are	33
As a form of photo identification	23.4
Refused to answer	18
Number of respondents	2,002

**Table B.47. Banks can offer a service whereby checks to be deposited are photographed using your camera phone and the image is sent over the mobile Internet during a mobile banking session so that the bank can deposit the funds into your account without you having to present the physical check. The bank then sends a notification acknowledging receipt of the deposit. If your bank offered this service, how likely would you be to use it?**

Percent, except as noted

Q47	
I already use it	3.9
Very likely	13.7
Somewhat likely	24.1
Somewhat unlikely	20.8
Very unlikely	36.4
Refused to answer	1.1
Number of respondents	2,002

**Table B.48. Before going to a retail store to make a large purchase, do you generally compare prices online?**

Percent, except as noted

Q48	
Yes	58.4
No	41.1
Refused to answer	0.4
Number of respondents	2,189

**Table B.49. Before going to a retail store to make a large purchase, do you generally look at product reviews online?**

Percent, except as noted

Q49	
Yes	57.6
No	41.6
Refused to answer	0.7
Number of respondents	2,189

**Table B.50. Online shopping is when you go to a merchant's website through your web browser or an application and make a purchase. Have you ever used your mobile phone for online shopping?**

Percent, except as noted

Q50	
Yes	16.4
No	82.3
Refused to answer	1.4
Number of respondents	2,002

**Table B.51. Have you ever used your mobile phone to comparison-shop over the Internet while at a retail store?**

Percent, except as noted

Q51	
Yes	19.4
No	79.4
Refused to answer	1.2
Number of respondents	2,002

**Table B.52. Have you ever used a barcode scanning application on your mobile phone while shopping at a retail store to find the best price for an item?**

Percent, except as noted

Q52	
Yes	12.3
No	86.7
Refused to answer	0.9
Number of respondents	2,002

**Table B.53. Has using your mobile phone to compare prices while you were shopping at a retail store ever changed where you made your purchase?**

Percent, except as noted

Q53	
Yes	65.6
No	34.4
Number of respondents	393

**Table B.54. Have you ever used your mobile phone to browse product reviews while shopping at a retail store?**

Percent, except as noted

Q54	
Yes	16
No	83.2
Refused to answer	0.7
Number of respondents	2,002

**Table B.58. Have you signed up to receive coupons or special offers by e-mail from retail stores in the past 12 months?**

Percent, except as noted

Q58	
Yes	37.9
No	60.7
Refused to answer	1.4
Number of respondents	2,290

**Table B.55. Has reading product reviews on your mobile phone while shopping at a retail store ever changed which item you ended up purchasing?**

Percent, except as noted

Q55	
Yes	76.9
No	22.5
Refused to answer	0.6
Number of respondents	289

**Table B.59. Have you made a purchase as a result of receiving one of these coupons or special offers?**

Percent, except as noted

Q59	
Yes	73.4
No	25.8
Refused to answer	0.8
Number of respondents	881

**Table B.56. In the past 12 months, have you used your mobile phone to check your account balance or available credit before making a large purchase?**

Percent, except as noted

Q56	
Yes	67.2
No	32.1
Refused to answer	0.7
Number of respondents	372

**Table B.60. Have you ever signed up to receive coupons/offers from a website such as Groupon or Living Social?**

Percent, except as noted

Q60	
Yes	28.2
No	70.5
Refused to answer	1.2
Number of respondents	2,290

**Table B.57. Thinking of the most recent time that you used your mobile phone to check your account balance or available credit before making a large purchase, did you decide not to buy that particular item because of the amount of money left in your account or the amount of your available credit?**

Percent, except as noted

Q57	
Yes	59.2
No	40.5
Refused to answer	0.3
Number of respondents	242

**Table B.61. Have you ever used a coupon from a website such as Groupon or Living Social?**

Percent, except as noted

Q61	
Yes	56.7
No	43.3
Number of respondents	657

**Table B.62. New mobile contactless payments are becoming available from some banks, credit card companies, and transit operators. These let consumers tap or wave their mobile phone at a terminal instead of swiping a card. If you were offered the option of using this service, how likely would you be to use it?**

Percent, except as noted

Q62	
I already use it	1
Very likely	9.9
Somewhat likely	23.1
Somewhat unlikely	22.4
Very unlikely	42.3
Refused to answer	1.3
Number of respondents	2,002

**Table B.63. How likely do you think it is that mobile contactless payments will become a major form of payment in the next five years?**

Percent, except as noted

Q63	
Very likely	16.7
Somewhat likely	33.3
Somewhat unlikely	15.5
Very unlikely	11.5
Don't know	21.8
Refused to answer	1.1
Number of respondents	2,002

**Table B.64. How much responsibility do you have for maintaining the household budget and managing household income?**

Percent, except as noted

Q64	
None or almost none	11.5
Some	10.9
Shared equally with other household members	26.9
Most	13
All or almost all	36.3
Refused to answer	1.3
Number of respondents	2,290

**Table B.65. How much responsibility do you have for paying monthly bills (e.g., rent or mortgage, utilities, cell phone)?**

Percent, except as noted

Q65	
None or almost none	15.2
Some	11.5
Shared equally with other household members	18.9
Most	10.8
All or almost all	42.1
Refused to answer	1.6
Number of respondents	2,290

**Table B.66. How much responsibility do you have for shopping for household goods and groceries?**

Percent, except as noted

Q66	
None or almost none	9.2
Some	16.3
Shared equally with other household members	24.8
Most	13.3
All or almost all	34.8
Refused to answer	1.7
Number of respondents	2,290

**Table B.67. How much responsibility do you have for making decisions about savings and investments?**

Percent, except as noted

Q67	
None or almost none	12.1
Some	9.9
Shared equally with other household members	35.4
Most	11.7
All or almost all	30
Refused to answer	0.9
Number of respondents	2,290

**Table B.68. Do you or anyone in your household use a program or website to track household finances (for example, Quicken, Mint.com, Excel, or a website provided by your bank)?**

Percent, except as noted

Q68	
Yes	21.3
No	78.1
Refused to answer	0.6
Number of respondents	2,290

**Table B.69. How long have you been using this program or website to manage your household finances?**

Percent, except as noted

Q69	
Less than a year	15.6
One to two years	17.9
Three to five years	22.9
More than five years	42.7
Refused to answer	0.8
<b>Number of respondents</b>	<b>514</b>

**Table B.72. What method(s) do you use to track purchases and expenses on your mobile phone?**

Percent, except as noted

Q72	
A mobile application for expense tracking	38.3
A spreadsheet	10.1
Online (using the web browser to access a website)	47.6
Send text messages	12.1
Take notes in a notepad or word processor	21.1
Refused to answer	3.4
<b>Number of respondents</b>	<b>115</b>

**Table B.70. In a typical month, how often do you or another household member use this program or website?**

Percent, except as noted

Q70	
0	3.3
1	12.6
2	10.4
3	7.1
4	11.5
5	6.3
6	2.9
7	0.6
8	3.1
10	6.5
12	1.8
14	0.4
15	4.8
20	6.4
21	0.1
24	0.2
25	5.8
26	0.5
27	0.2
30	7.7
31	0.2
35	0.5
40	0.3
45	0.1
50	0.9
60	0.3
Refused to answer	5.4
<b>Number of respondents</b>	<b>514</b>

**Table B.73. In a typical month, how often do you use your mobile phone to track purchases and expenses?**

Percent, except as noted

Q73	
0	2.9
1	2.7
2	16.6
3	10.4
4	5.4
5	15.4
6	0.8
7	0.3
8	0.5
10	5.8
12	0.4
13	0.1
14	0.4
15	8.8
20	7.5
25	2.8
30	4.2
40	2.1
50	0.3
123	0.2
Refused to answer	12.6
<b>Number of respondents</b>	<b>115</b>

**Table B.71. Do you use your mobile phone to track purchases and expenses?**

Percent, except as noted

Q71	
Yes	7.3
No	91.7
Refused to answer	1
<b>Number of respondents</b>	<b>2,002</b>

**Table B.74. You previously mentioned that you receive text alerts from your bank. What kind of text alerts do you receive?**

Percent, except as noted

Q74	
Low-balance alerts	66.4
Payment due alerts	31.7
Saving reminders	3.1
Fraud alerts	30.3
Other	18.2
<b>Number of respondents</b>	<b>111</b>

**Table B.75. Thinking of the most recent low-balance alert you received by text message, which of the following actions did you take after receiving the alert?**

Percent, except as noted

Q75	
Transferred money into the account with the low balance	57.6
Deposited money into the account with the low balance	16.2
Reduced my spending	41.1
None of the above	15.9
<b>Number of respondents</b>	<b>78</b>

**Table B.79. If an investor who only owns two stocks right now decides to instead spread their money among many different assets (i.e., more stocks, add bonds, add real estate), their risk of losing money on their entire portfolio will do what?**

Percent, except as noted

Q79	
Increase	21
Decrease	52.4
Stay the same	22.5
Refused to answer	4.1
<b>Number of respondents</b>	<b>2,290</b>

**Table B.76. Has receiving payment due alerts improved your ability to pay your bills on time?**

Percent, except as noted

Q76	
Yes, by a lot	37.4
Yes, by a little	40.4
No	22.2
<b>Number of respondents</b>	<b>41</b>

**Table B.80. If you were to invest \$1,000 in a stock mutual fund for a year, it would be possible to have less than \$1,000 when you withdraw your money.**

Percent, except as noted

Q80	
True	76
False	20.3
Refused to answer	3.6
<b>Number of respondents</b>	<b>2,290</b>

**Table B.77. Imagine that the interest rate on your savings account was 1 percent per year and inflation was 2 percent per year. After one year, how much would you be able to buy with the money in this account?**

Percent, except as noted

Q77	
More than today	5.6
Exactly the same	20.9
Less than today	70.4
Refused to answer	3
<b>Number of respondents</b>	<b>2,290</b>

**Table B.81. Suppose you owe \$1,000 on a loan and the interest rate you are charged is 10 percent per year compounded annually. If you didn't make any payments on this loan, at this interest rate, how many years would it take for the amount you owe to double?**

Percent, except as noted

Q81	
Less than two years	11.7
Between two and five years	23.8
Five to nine years	34.2
Ten years or more	25.8
Refused to answer	4.5
<b>Number of respondents</b>	<b>2,290</b>

**Table B.78. Considering a long time period (for example, 10 or 20 years), which asset normally gives the highest return?**

Percent, except as noted

Q78	
Savings accounts	15.3
U.S. Government bonds	25
Stocks	55.8
Refused to answer	3.9
<b>Number of respondents</b>	<b>2,290</b>

**Table B.82. Imagine that your car breaks down and requires \$400 worth of repairs in order to drive again. Based on your current financial situation, how would you pay for this expense? If you would use more than one method to cover this expense, please select all that apply.**

Percent, except as noted

Q82	
Put it on my credit card	36.4
With the money currently in my checking account	40.8
By taking money out of my savings	21.5
Using money from a bank loan, line of credit, or overdraft	3.4
By borrowing from a friend or family member	17.5
Using a payday loan or deposit advance	2.9
By pawning something	6
Other	5.7
Refused to answer	2.9
Number of respondents	2,290

**Table B.83. Which of the following statements comes closest to describing the amount of financial risk that you are willing to take when you save or make investments?**

Percent, except as noted

Q83	
Take substantial financial risks expecting to earn substantial returns	3.3
Take above average financial risks expecting to earn above average returns	14.6
Take average financial risks expecting to earn average returns	36.9
Not willing to take any financial risks	42.5
Refused to answer	2.6
Number of respondents	2,290

**Table B.84. Suppose that you are the only income earner in the family, and you have a good job guaranteed to give you your current income every year for life. You are given the opportunity to take a new and equally good job, with a 50–50 chance that it will double your income and a 50–50 chance that it will cut your income by one-third (33 percent). Would you take the new job?**

Percent, except as noted

Q84	
Yes	24.1
No	73
Refused to answer	2.9
Number of respondents	2,290

**Table B.85. Now suppose that the chances were 50–50 that it would double your income and 50–50 that it would cut your income by half (50 percent). Would you still take the new job?**

Percent, except as noted

Q85	
Yes	36.2
No	63.1
Refused to answer	0.7
Number of respondents	547

**Table B.86. Now suppose that the chances were 50–50 that it would double your income and 50–50 that it would cut your income by one-fifth (20 percent). Would you now take the new job?**

Percent, except as noted

Q86	
Yes	22.5
No	76.8
Refused to answer	0.7
Number of respondents	1,687

**Table B.87. Summary Statistics for Demographics**

	Mean	Standard Deviation
Age	46.6209	16.9178
Male	0.4841	0.4999
Female	0.5159	0.4999
Ages 18–29	0.2139	0.4101
Ages 30–44	0.2569	0.4387
Ages 45–60	0.2765	0.4469
Ages over 60	0.2507	0.4335
Less than high school	0.1267	0.3327
High school degree	0.3035	0.4599
Some college	0.2875	0.4527
Bachelor's degree or higher	0.2822	0.4502
White, non-Hispanic	0.6795	0.4668
Black, non-Hispanic	0.1158	0.3200
Other and two or more races, non-Hispanic	0.0679	0.2516
Hispanic	0.1369	0.3438
Less than \$25,000	0.2154	0.4112
\$25,000–\$39,999	0.1734	0.3787
\$40,000–\$74,999	0.2623	0.4400
\$75,000–\$99,999	0.1293	0.3356
Greater than \$100,000	0.2195	0.4140
Married	0.5279	0.4993
Unmarried, widowed, divorced, or living with partner	0.4721	0.4993
Northeast	0.1842	0.3877
Midwest	0.2174	0.4126
South	0.3659	0.4818
West	0.2324	0.4225
Employed	0.5559	0.4970
Unemployed but in labor force	0.0970	0.2961
Not in labor force: retired, disability or other	0.3470	0.4761
Observations	2,290	

**Table B.88. Use of online banking on a desktop, laptop, or tablet computer in the past 12 months by age**

Percent, except as noted

Age categories	Yes	No	Total
18-29	24.6	10.6	20.1
30-44	30.4	16.8	26
45-59	24.7	32.5	27.2
60+	20.3	40.1	26.7
Number of respondents	1,358	644	2,002

**Table B.89. Use of mobile banking in the past 12 months by age**

Percent, except as noted

Age categories	Yes	No	Total
18-29	43.5	16.8	22.4
30-44	35.7	24.7	27
45-59	14.7	30.2	26.9
60+	6.1	28.4	23.7
Number of respondents	372	1,626	1,998

**Table B.90. Use of mobile payments in the past 12 months by age**

Percent, except as noted

Age categories	Yes	No	Total
18-29	37.3	20.3	22.4
30-44	35.9	25.6	26.9
45-59	16.9	28.5	27
60+	10	25.7	23.7
Number of respondents	213	1,780	1,993

**Table B.91. Use of online banking on a desktop, laptop, or tablet computer in the past 12 months by race**

Percent, except as noted

Race/ethnicity	Yes	No	Total
White, Non-Hispanic	73.3	68.8	71.8
Black, Non-Hispanic	7.6	13.4	9.4
Other, Non-Hispanic	5.7	4.8	5.4
Hispanic	12.4	12.2	12.3
2+ Races, Non-Hispanic	1.1	0.7	1
Number of respondents	1,358	644	2,002

**Table B.92. Use of mobile banking in the past 12 months by race**

Percent, except as noted

Race/ethnicity	Yes	No	Total
White, Non-Hispanic	60.3	71.5	69.2
Black, Non-Hispanic	16.2	10	11.3
Other, Non-Hispanic	5.2	5.8	5.6
Hispanic	17.1	11.6	12.8
2+ Races, Non-Hispanic	1.2	1.1	1.2
Number of respondents	372	1,626	1,998

**Table B.93. Use of mobile payments in the past 12 months by race**

Percent, except as noted

Race/ethnicity	Yes	No	Total
White, Non-Hispanic	58.3	70.8	69.3
Black, Non-Hispanic	12.9	10.9	11.2
Other, Non-Hispanic	7.1	5.4	5.6
Hispanic	20.9	11.6	12.8
2+ Races, Non-Hispanic	0.9	1.2	1.2
Number of respondents	213	1,780	1,993

**Table B.94. Use of online banking on a desktop, laptop, or tablet computer in the past 12 months by gender**

Percent, except as noted

Gender	Yes	No	Total
Female	51.9	52.3	52.1
Male	48.1	47.7	47.9
Number of respondents	1,358	644	2,002

**Table B.95. Use of mobile banking in the past 12 months by gender**

Percent, except as noted

Gender	Yes	No	Total
Female	53.4	52.9	53
Male	46.6	47.1	47
Number of respondents	372	1,626	1,998

**Table B.96. Use of mobile payments in the past 12 months by gender**

Percent, except as noted

Gender	Yes	No	Total
Female	55	52.7	53
Male	45	47.3	47
Number of respondents	213	1,780	1,993

**Table B.97. Use of online banking on a desktop, laptop, or tablet computer in the past 12 months by education group**  
Percent, except as noted

Education	Yes	No	Total
Less than high school	5.2	16.7	8.9
High school	23.1	41.3	29
Some college	32.9	25.1	30.4
Bachelor's degree or higher	38.8	16.9	31.8
<b>Number of respondents</b>	<b>1,358</b>	<b>644</b>	<b>2,002</b>

**Table B.100. Use of online banking on a desktop, laptop, or tablet computer in the past 12 months by income group**  
Percent, except as noted

Income group	Yes	No	Total
Less than \$25,000	10.1	27.1	15.6
\$25,000–\$39,999	17.2	19.3	17.9
\$40,000–\$74,999	28.5	27.1	28.1
\$75,000–\$99,999	15.9	11	14.4
\$100,000 or greater	28.2	15.5	24.2
<b>Number of respondents</b>	<b>1,358</b>	<b>644</b>	<b>2,002</b>

**Table B.98. Use of mobile banking in the past 12 months by education group**  
Percent, except as noted

Education	Yes	No	Total
Less than high school	5.5	12.1	10.7
High school	21.5	31.8	29.6
Some college	39	27.4	29.8
Bachelor's degree or higher	34	28.8	29.9
<b>Number of respondents</b>	<b>372</b>	<b>1,626</b>	<b>1,998</b>

**Table B.101. Use of mobile banking in the past 12 months by income group**  
Percent, except as noted

Income group	Yes	No	Total
Less than \$25,000	12.8	19.9	18.4
\$25,000–\$39,999	19	16.6	17.1
\$40,000–\$74,999	27.5	26.5	26.7
\$75,000–\$99,999	12.9	14	13.8
\$100,000 or greater	27.9	22.9	24
<b>Number of respondents</b>	<b>372</b>	<b>1,626</b>	<b>1,998</b>

**Table B.99. Use of mobile payments in the past 12 months by education group**  
Percent, except as noted

Education	Yes	No	Total
Less than high school	7.2	11.2	10.7
High school	27.9	29.9	29.7
Some college	37	28.7	29.7
Bachelor's degree or higher	27.9	30.1	29.9
<b>Number of respondents</b>	<b>213</b>	<b>1,780</b>	<b>1,993</b>

**Table B.102. Use of mobile payments in the past 12 months by income group**  
Percent, except as noted

Income group	Yes	No	Total
Less than \$25,000	19.1	18.5	18.5
\$25,000–\$39,999	20.6	16.7	17.2
\$40,000–\$74,999	23	27.2	26.7
\$75,000–\$99,999	11.7	14	13.7
\$100,000 or greater	25.6	23.6	23.9
<b>Number of respondents</b>	<b>213</b>	<b>1,780</b>	<b>1,993</b>



**RESPONSES TO WRITTEN QUESTIONS OF SENATOR KIRK  
FROM SANDRA F. BRAUNSTEIN**

**Q.1.** Now that the Federal Government will be participating in the Automated Clearing House to distribute Government benefits like social security, growth trends for electronic payments should accelerate at an even faster pace going forward than the double-digit increases we have seen for the past few years. Please describe your perspective of role the Federal Reserve should play in regulating and facilitating electronic payments in the post- Dodd-Frank world, with an emphasis on how the Federal Reserve can contribute to maximizing the economic benefits of new technology.

**A.1.** Federal Government benefits have for decades been provided through automated clearing house (ACH), or “direct deposit,” payments to beneficiaries’ accounts at depository institutions, and for many years the vast majority of benefit payments have been made in this manner, rather than by check. Making the payments electronically is generally less expensive, faster, and more secure than making them by check. For example, delivery of paper checks to benefit recipients may be delayed, and the checks, once received, may be lost, misplaced, or stolen.

In December 2010, the U.S. Treasury issued a rule to increase further the usage of electronic payments for the disbursement of Government benefits. The rule requires anyone applying for benefits on or after May 2011 to receive all payments electronically via direct deposit to a deposit account at a depository institution or via a prepaid card. Treasury has contracted with a commercial bank to make Direct Express® Debit MasterCard® prepaid card accounts available to recipients who will not be receiving benefits via direct deposit; these cards can be used like other debit cards, and funds that recipients receive through the card are FDIC insured. There is no cost to sign up for the card and no monthly fee, although there are fees for some optional transactions (such as making more than one ATM withdrawal in a single month). The Direct Express® card enables benefit recipients who do not have bank accounts to avoid fees associated with cashing benefit checks. Recipients currently receiving benefits via checks will be required to switch to an electronic payment method by March 2013.

Also in December 2010, the U.S. Treasury issued a rule establishing requirements that apply to the delivery of Federal payments to prepaid cards other than the Direct Express® card. Under the rule, a prepaid card is eligible to receive Federal payments only if the card account is Federally insured, the card is not attached to a line of credit or loan agreement under which repayment from the account is triggered upon delivery of the Federal payments, and the issuer of the card provides the cardholder with all of the consumer protections that apply to a payroll card account under Regulation E (12 CFR part 1005).

With respect to benefits that are received on a Direct Express® card or prepaid card meeting Treasury’s requirements, Regulation E (12 CFR part 1005), which implements the Electronic Fund Transfer Act of 1978 (EFTA), limits a recipient’s liability for unauthorized electronic fund transfers out of the recipient’s benefit account (*e.g.*, if the card is lost or stolen). The Dodd-Frank Act transferred the Board’s rule-writing authority with respect to most con-

consumer protection laws, including most of the EFTA, to the Consumer Financial Protection Bureau. Under Regulation E, cardholders who dispute a transaction within 2 business days of learning of the loss or theft of their card cannot be held liable for more than \$50. Those who dispute a charge within 60 days of an account statement reflecting the unauthorized transfer cannot be held liable for more than \$500. Finally, the regulation provides consumers with specific error-resolution rights in the case of an unauthorized transaction.

The Nation's retail payment system is becoming increasingly electronic, largely reflecting consumer preferences. The Federal Reserve continues to promote the safety and efficiency of the Nation's payments system through the Reserve Banks' role as providers of payment services and the Board's regulatory role. In addition, the Federal Reserve will work cooperatively with the private sector to identify and remove barriers to innovation and efficiency. And, finally, when appropriate, the Federal Reserve will act as a catalyst to greater efficiency, safety, and accessibility within the payments system.

**Q.2.** Sweden, the first European country to circulate bank note currency in 1661, is at the forefront of the move to a cashless economy. Its aggressive move to electronic transactions has resulted in a dramatic drop in robberies of banks and securities trucks and shrinkage of the "tax gap." Has the Federal Reserve quantified the costs reductions and economic benefit derived from migrating to mobile/Web payments?

**A.2.** The cost reductions and economic benefits derived generally from migrating paper-based payments to electronic payments have been supported by theoretical analysis and some empirical verification. For instance, the Federal Reserve Bank of Philadelphia issued a 2003 working paper showing that the shift from paper-based payments to electronic payments and from branch offices to ATMs may result in an annual costs savings of 1 percent of the gross domestic product.<sup>1</sup> Over a 10-year period, the Federal Reserve has reduced the cost of per-item processing by one third through the electronic clearing of paper checks.

For mobile payments specifically, the benefits in relation to costs are uncertain. The United States has a well-developed and efficient payments system and enabling mobile payments requires investments by the consumers' banks, merchants, and others. Research, however, also suggests that the long-term benefits to society of having a convenient, effective mobile wallet with complementary services that go beyond mobile payments (for instance, the ability to receive targeted ads and promotions and to monitor and manage account balances from any location) could be significant.

In terms of the example of Sweden's move to a "cashless economy," it may be helpful to provide some perspective from Sweden's central bank, the Riksbank. The Riksbank reports that cash and cards are the dominant payment methods used in Sweden today at the point of sale. The Riksbank data show that cash usage has decreased since the 1950s, but that trend has been driven by an in-

<sup>1</sup>"Cost Savings From Electronic Payments and ATMs in Europe", August 2003, Working Paper No. 03-16, at <http://www.frbatlanta.org/filelegacvdocs/epconfhumphrey.pdf>.

crease in card-based payments; neither e-money nor mobile payments are yet well established in Sweden. In addition, the decline in bank robberies in recent years has been driven primarily by changes in technology and operations. Specifically, the amount of cash in the bank offices has been reduced and replaced by deposit machines and automated teller machines. Also, the shrinkage of the tax gap has been affected by recent legislation that requires companies to have certified cash registers and to offer customers a receipt, which makes cheating on cash accounting much more difficult. Carriers have taken actions to increase safety, including GPS systems in cars and cash bags, improved ink security systems in vehicle safes and cash bags, personnel training, and stricter screening of cash transporters. Despite these actions, armored carrier robberies have increased. The Riksbank believes that the cash usage will continue to decrease but that cash nevertheless will continue to be a prominent means of payment for the foreseeable future. The impact of new methods of payment, such as mobile payments, on the future demand for cash in Sweden is uncertain.

**Q.3.** The “Consumers and Mobile Financial Services” report issued by the Board of Governors in March 2012 concludes that the consumers’ doubts about the security of mobile financial transactions impede the growth of this new technology. What concrete recommendation would you make to improve mobile security for financial stakeholders as well as consumers? At the same time, what steps should be taken to assure that privacy rights are protected? Please identify all stakeholders that need to be considered, and all regulatory agencies that will be involved.

**A.3.** It is important that multiple stakeholders involved in a mobile payment transaction share responsibility for ensuring mobile payment security and protecting consumer privacy rights. Stakeholders include mobile carriers that sell and enable mobile phones for payments and oversee the handset and chip manufacturers’ security requirements, financial institutions that issue debit and credit cards and/or hold consumer bank accounts that are accessed from the mobile wallets, card networks (debit, credit, and prepaid), mobile solution providers, merchants, and consumers. This nascent market would benefit from mobile stakeholders jointly developing technological standards and guidelines that support different mobile payment technologies and alternatives to prevent attacks on mobile payment data and facilitate the development and implementation of consistent, integrated security measures. For example, mobile stakeholders should collaborate to develop an effective mobile payments security program that applies appropriate security measures and tools. Such a program could—

- Include a simple customer security toolkit showing consumers how to protect their mobile devices, mobile wallets, and payments data by using antivirus software to ensure the applications downloaded are safe from viruses and malware; creating passwords for login and mobile wallet access; loading software that enables the phone to be remotely wiped, locked, or deactivated if lost or stolen; and detecting and reporting fraud or other security breaches.

- Recommend implementation of appropriate security tools for different mobile technologies, including the use of end-to-end encryption for any mobile payment transaction stored on the phone, remotely on a file server, and when data are in transit over the wireless network to protect consumer personal data (bank account and card numbers and passwords).
- Create a certification process and standard procedures to safely set-up mobile phones and wallets, including certifying vendor applications before they are loaded into mobile wallets and certifying wallets before they are put into the secure container in the phone. Certification and testing will help to ensure that data processed are encrypted and safely stored, and that applications are virus and malware free.

From a privacy perspective, mobile stakeholders should pursue jointly developing best practices that identify, standardize, and build controls that protect consumer data on mobile phones and address transparency and choice. Smartphones enable mobile payment apps to capture a broad range of user information automatically, including a consumer's geolocation, phone number, contact list, call logs, unique IDs, and other data stored on the device. In addition to protecting against security breaches, industry could develop business practices for using and sharing this data, within applicable statutory and regulatory requirements. As initial steps, it could be helpful to review the Federal Trade Commission (FTC), Mobile Marketing Association (MMA), and other privacy guidelines developed to help protect consumer privacy in the mobile space, with emphasis on transparency, disclosures, consumer choice, and education.<sup>2</sup> It also could be helpful to inventory best practices in the United States and globally to ensure that they include strong privacy protections that encompass the entire mobile stakeholder community and address transparency, consumer education, and consumer choice. Consumers should understand their rights and obligations when they make mobile payments, especially with multiple parties involved in a mobile transaction. Mobile payment companies also should give consumers the ability to restrict using or sharing any information that is not necessary to complete a transaction.

Further analysis of existing laws may be needed to ensure that consumers are adequately protected. A legal framework exists to address the payment activities of insured depository institutions—collectively, “banks.” This framework includes consumer protection statutes, such as the Gramm-Leach-Bliley Act’s privacy provisions, the Electronic Fund Transfer Act (EFTA), and the Truth in Lending Act, as well as the bank supervisory process. To the extent that nonbanks are involved, whether and the degree to which Federal or State statutes and rules are applicable depends on the nonbank’s role in the transaction and the specific provisions of the particular statute or rule. Due to the different types of service pro-

<sup>2</sup>In May 2012, the FTC issued a report on *Protecting Consumer Privacy in an Era of Rapid Change*, which identified best practices for businesses to protect consumer privacy and give them greater control over the collection and use of their personal data and urged mobile providers to work toward improved privacy protections, including disclosures. In December 2011, the MMA published its *Mobile Application Privacy Policy Framework*, which addressed privacy issues and data processes of many, but not all, mobile applications.

viders (bank and nonbank) and the wide variety of payment arrangements that are in place and under development, a number of regulators may have authority over various aspects of mobile payment transaction, including the Federal bank regulators, the Consumer Financial Protection Bureau, the Federal Trade Commission, the Federal Communications Commission, the Treasury Department's Financial Crimes Enforcement Network, and State agencies. However, given the fast-paced nature of changes in this area and the potential for significant improvements in consumer financial services through mobile payments, further fact-finding would aid that analysis and would be helpful to ensure that any legislative or regulatory proposals do not stifle the very innovations that would benefit consumers overall.

It is important that mobile payment stakeholders and public agencies take steps to develop coordinated programs for consumer education and awareness related to securing mobile payments and protecting consumer privacy. For example, the Federal Reserve Bank of Boston Payments staff will continue to work with mobile payment stakeholders through the Mobile Payments Industry Workgroup to help facilitate such security and privacy initiatives.<sup>3</sup>

**Q.4.** In its 2011 Annual Report of Competitive Market Conditions, the FCC cited forecasts that more than half the Nation will use smart phones to conduct numerous banking transactions by 2015; among consumers between the age of 18 and 35, over three-quarters of them will bank by mobile device. Do you agree with the FCC projections?

**A.4.** Smartphone usage is increasing rapidly in the United States. The Board's recent *Consumers and Mobile Financial Services* survey found that just under 40 percent of Americans between the ages of 18 and 35 were smartphone users in December of 2011. Smartphone users are much more likely to use mobile banking than other mobile phone users: among those consumers between the ages of 18 and 35, 56 percent of smartphone users had used mobile banking in the past 12 months compared to 11 percent of nonsmartphone users.<sup>4</sup> As more and more consumers have smartphones and the number of financial institutions offering mobile banking and mobile payment services increase, it is reasonable to assume that the proportion of the population that use these services will also increase. However, although Federal Reserve and industry data can help us understand directional trends, it is more difficult to project the specific future penetration rate for these mobile financial services.

**Q.5.** According to surveys within the "Consumers and Mobile Financial Services" report, the 11 percent of the adult population classified as "underbanked" are more dependent on mobile services than the general population; almost two-thirds of "underbanked" pay bills with their mobile phones to pay bills, compared to less than half of all mobile phone users. In the final words of this re-

<sup>3</sup>The Mobile Payments Industry Workgroup represents major mobile payment stakeholders, including mobile carriers, banks, card networks, payment processors, Internet payment providers, mobile chip manufacturers, mobile solution providers, merchants, and mobile and payment trade associations.

<sup>4</sup>Pursuant to the data collected in the Board of Governors of the Federal Reserve System *Consumers and Mobile Financial Services* survey.

port, “The prevalence of mobile phone access among minorities, low-income individuals, and younger generations creates the possibility of using mobile technology to expand financial inclusion.” Since 23 of the top 25 banks offer mobile banking, should we modify regulation of community development and investment initiatives to include expansion of mobile services, accompanied by security protocols and consumer awareness programs?

**A.5.** The manner in which traditionally underbanked consumers may be accessing mobile financial services is an interesting aspect of the report. Because the technology and business models are so new and still evolving, it is unclear to what extent mobile services may ultimately complement, augment, or supplant more traditional means of delivering financial services to consumers, including consumers without banking relationships and those who are banked but also use alternative financial services. The Federal Reserve will continue to monitor this aspect of the marketplace. Given the still-evolving nature of the technology, it may be too soon to consider statutory or regulatory changes. Changes such as those you suggest may be warranted in the future if they would be effective to expand financial inclusion through the offerings of mobile products and services.

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

**MOBILE PAYMENTS IN THE UNITED STATES: MAPPING OUT THE ROAD  
AHEAD**

**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**

---

---

The authors would like to thank the members of the Mobile Payments Industry Workgroup for their valuable contributions to the work effort and insightful ideas and comments that are the foundation of this paper. The views expressed in this paper are solely those of the authors and do not reflect official positions of the Federal Reserve Banks of Atlanta or Boston or the Federal Reserve System.

## I. Executive Summary

In January 2010, the Federal Reserve Banks of Atlanta and Boston, through their Retail Payments Risk Forum and Payments Research groups, convened a selected set of key players in this country's emerging mobile payments ecosystem. The goal of the meeting was to facilitate a discussion among all involved parties as to how a successful mobile payments (as opposed to mobile banking) regimen could evolve in the U.S.

Over the past 15 months, the self-named Mobile Payments Industry Workgroup (MPIW)<sup>1</sup> met five times to share information and ideas, discuss the barriers and opportunities resident in mobile payments, and ultimately, to suggest a vision for the building blocks of an efficient and ubiquitous mobile payments environment. Ultimately, the discussions of this group, along with additional industry dialogue and literature research, constituted a body of input to the development of a research paper regarding the future for point-of-sale (POS) mobile payments in the United States.

This paper, drafted by the Boston and Atlanta Reserve Bank payments research teams, does not necessarily reflect the opinions of the Federal Reserve Banks, the opinion of the Federal Reserve Board of Governors, or the opinion of any individual member of the workgroup. Rather, the paper represents the collective views of the authors based on the inputs noted above. The paper depicts the current mobile payments ecosystem in the U.S.; discusses barriers, gaps, and opportunities; and sets forth a set of foundational elements that workgroup participants believe are fundamental to the development of a robust mobile payments environment. This "vision" for the future is built upon the recognition that the current environment faces many challenges and that success will require extensive collaboration between participants to ensure that consumers see a homogenous solution as they do today in other payment channels such as checks, ACH, and cards. Moreover, it must be a solution based on agreed upon standards, rules, and practices that ensure seamless interoperability regardless of the handset, mobile carrier, financial institution, payment network, or merchant location involved in any individual's desired transaction.

The foundational components of success suggested by the work group include:

1. The proposed environment is best defined by the concept of an "open mobile wallet."
2. The mobile infrastructure would likely be based on Near Field Communications (NFC) contactless technology resident in a smart phone and merchant terminals.

---

<sup>1</sup> Use of the MPIW in this paper represents the existing workgroup or a modified version of the group in the future.

3. Ubiquitous platforms for mobile should leverage existing rails, including the ACH network for non-card payments, and support new payment types that meet emerging needs.
4. Some form of dynamic data authentication would be at the heart of a layered mobile payments security and fraud mitigation program.
5. Standards would be designed, adopted, and complied with through an industry certification program to ensure both domestic and global interoperability, including a standard to ensure that devices used to facilitate mobile payments do not create any electronic interference problems.
6. A better understanding of a regulatory oversight model should be developed in concert with bank and non-bank regulators early in the effort to clarify compliance responsibilities.
7. Trusted Service Managers should oversee the provision of interoperable and shared security elements used in the mobile phone.

During their discussions, the MPIW debated the need for a new entity in the ecosystem directed at assisting the various parties to resolve issues of mutual concern and codify solutions in such a way as to facilitate interoperability and ubiquity. While many members felt that such an entity may be useful in the future, the general sense was that it was too early in the evolution to fully understand how such an entity might be constituted and what its role might be. In the meantime, the MPIW indicated a desire to meet again, perhaps with some additional attendees, to continue to discuss issues resident in the foundational components discussed above.

Additionally, the group discussed the need for an industry “roadmap” that could focus short term investment and accelerate progress. Once again, the general sense was that the complexity of the environment and diversity of participants would make this a daunting task. Efforts to specifically prescribe such a roadmap could create results that are inconsistent with the outcome eventually produced from natural market forces. Therefore, the group decided that defining such a roadmap this early in evolution of mobile payments in the U.S. might stifle innovation.

The benefits of this document and the underlying participative work effort will be revealed by what happens next. This paper is intended to be a vehicle for socializing a concept or model for an efficient, secure, ubiquitous, and convenient mobile payments evolution in this country to a much broader group of industry players. They, in turn, must ultimately agree to support or modify the ideas contained herein as a means of moving forward, recognizing that the opportunity to achieve maximum benefits may be best realized by acting sooner, rather than later.

The ability of the two convening Reserve Banks to organize and facilitate the discussions that led to the publication of this document, in addition to the ongoing and highly engaged participation of a diverse group of mobile ecosystem players, speaks to the potential success of idea-sharing and demonstrates that

collaborative efforts could work. The authors would like to thank all the participants for their engagement and contributions to this work. A note of special thanks goes to Steve Mott of BetterBuyDesign, who contributed heavily to this effort.

## II. Introduction

Almost daily a new mobile payments venture is announced that makes it possible for a consumer or business to use mobile phone technology to enable or enhance the payment process. Initially, the focus has been on enabling a mobile device to be used as a browser, accessing existing internet-based banking and retail systems. More recently, attention has turned to the use of an application-enabled mobile phone as a payment form factor, substituting for a check, cash or a card to eventually create a mobile virtual wallet. Financial institutions are testing these capabilities, as are numerous non-banks, including some who operate in the internet space.<sup>2</sup> In some cases, the phone is simply used to initiate a card payment, but in other cases it is used to create a direct transfer to another individual or business using an existing bank-centric clearing and settlement capability (e.g. ACH), or an online payment service provider. Another variation embraces the concept of sending SMS (text) messages via mobile phone carriers, who perform the clearing and settlement function, as experienced in the successful program to funnel aid to Haiti in the wake of its earthquake disaster.

The concept of mobile banking and payments has resonated in many developing countries where lack of a physical banking or payments infrastructure exists.<sup>3</sup> Mobile payments have enabled financial inclusion for individuals and small businesses that are more remote from banks to overcome the limitations of physical transportation and utility systems. Mobile payments have even created a new currency in the form of airtime minutes. The evolution of mobile payments in the U.S. has followed a different path because of the well-defined banking and payments infrastructure already in place in the U.S. As a result, U.S. mobile payments have advanced more slowly; and many pilots, while conceptually interesting and educational, have failed to produce evidence of a currently sustainable business case. U.S. consumers are fortunate to have many different payment methods available to them, so the need for a fully deployed mobile payments alternative is not as obvious. Additionally, the cost of deploying the physical software and hardware elements of a ubiquitous mobile infrastructure is significant and must be justified in the face of uncertain consumer demand.

Nevertheless, there is growing evidence that mobile payments will become a significant element in the U.S. payments landscape in the future. A recent government report estimated that 18 percent of U. S.

---

<sup>2</sup> For example, Google, Amazon and PayPal, all who accept payments for internet purchases, are involved in mobile payments.

<sup>3</sup> Merritt, Cindy. 2010. "Mobile Money Transfer," Retail Payments Risk Forum, Federal Reserve Bank of Atlanta, September.

households do not have a bank account<sup>4</sup>, a key variable in the attractiveness of mobile payments in countries where the majority of the population is unbanked. However, in the U.S. it is not anticipated that the unbanked will be the take-off point for mobile payments. It is likely to be the smart phone user. About 34 percent of U.S. consumers now own a smart phone and that number is growing at a compound annual growth rate of 17 percent<sup>5</sup>. Most large U.S. banks offer customized banking applications for smart phones. Contactless mobile<sup>6</sup> technology provides additional capabilities resident in chips that can reduce payments fraud and potentially the cost that merchants bear to ensure their card brands are PCI compliant. Finally, the U.S. continues to become a more mobile society where consumers are motivated to use their time wisely. All of these factors point to the potential success of mobile-based payments and related activities in the future.

Most firms that would benefit from the long term deployment of mobile payments are eager to understand the details associated with successfully deploying a mobile payments infrastructure and accelerating progress wherever possible. Consequently, the Retail Payments Risk Forum at the Federal Reserve Bank of Atlanta<sup>7</sup> and the Payments Research Group at the Federal Reserve Bank of Boston<sup>8</sup> have collaborated to provide a setting for mobile industry participants to meet and discuss ways to move forward. This Mobile Payments Industry Workgroup (MPIW) is comprised of organizations representing the end-to-end mobile value chain. Since early 2010 they have met quarterly to discuss the reality of mobile payments and discern the way forward. Many of the discussions were first time events involving participants who had not previously engaged in face-to-face conversations, yet through this process some agreement has been reached on a number of key variables applicable to a perceived formula for mobile payments success in the U.S.

Present at the meetings were mobile carriers, issuing and acquiring banks, card brands, payments processors, credential manufacturers, trade associations (including merchants), mobile software solution vendors, handset makers, and large online payment service providers. To focus the discussion of “what is possible,” the participants learned more about each other’s business propositions, engaged in group activities aimed at understanding what cost and revenue factors were present, discussed various barriers to success, and contributed input to a basic set of characteristics that would be common to a successful mobile payments architecture.

---

<sup>4</sup> FDIC. 2009. “National Survey of Unbanked and Underbanked Households,” December.

<sup>5</sup> Javelin Strategy & Research. 2011. “Mobile Wallets: With the New Mobile Network Operator Joint Venture Isis, Are Cards and Cash Ready to go Mobile in 2011?” January.

<sup>6</sup> Contactless mobile and mobile NFC will be used interchangeably throughout this paper.

<sup>7</sup> <http://www.frbatlanta.org/rprf/>

<sup>8</sup> <http://www.bostonfed.org/economic/cprc/index.htm>

These discussions occurred in a very dynamic U.S. payments environment. Even as the MPIW was meeting, new mobile pilot programs were announced (some involving workgroup participants), the Durbin Amendment to the Financial Reform Act was adopted, other new mobile technologies were launched, and an initial interchange price regimen was proposed by the Federal Reserve Board of Governors. Nevertheless, the focus of the group has been on long run success in the creation of a profitable and ubiquitous mobile payments infrastructure. The chicken and egg challenges of merchant deployment and consumer usage were debated, the roles of banks and telecoms clarified, and different infrastructure models were discussed. Ultimately, it became clear that significant success was likely to come as a result of collaboration directed at identifying necessary standards and encouraging efficient implementations, rather than independent action.

In essence, this paper is intended to be a framework for more widespread industry discussion and debate that could lead to more sustainable progress in improving overall U.S. payments system efficiency and integrity than might occur otherwise. In the sections that follow, we define the composition of the mobile ecosystem, describe a vision for a successful implementation, address the potential benefits and drawbacks of mobile deployment, outline the obstacles and barriers to be addressed, identify the components of an industry business case, set forth key standards issues for discussion, explore various use case scenarios, and propose possible directions moving forward.

Ultimately, the value of this work lies in its overall acceptance and use, recognizing that the payments system environment today, while stable and secure, may be affected by any number of factors, including the broad spate of legal/regulatory activity emanating from Congress, therefore making it difficult to move to a single agenda.

The MPIW realized that there are various terms used in the mobile ecosystem that need to be explained or clarified. Consequently, we have included a glossary of key terms in Appendix I.

### **III. U.S. Mobile Payments Infrastructure Today**

While mobile payments, as opposed to mobile banking, applications have gained notable recent success in other parts of the world, they are just beginning to emerge in the U.S. Mobile payments for physical goods and services (e.g. POS and transit) imply the use of near field communications (NFC) contactless technologies that are not yet prevalent in the U.S., even in the card world. While NFC-like contactless technologies (e.g. barcodes, stickers, micro SD chips) have been appearing in the market recently, the emerging common standard for POS mobile transactions is near field communication (NFC). NFC enables a transmission using a very short-range wireless connectivity technology with the capacity to execute payment transactions, and a secure element that securely stores information such as identity

credentials and financial value. The appeal of NFC is that it is compatible and interoperable with other current systems, e.g. transit and security. In essence, it is not a new technology and works with existing hardware, secure elements and communication protocols.<sup>9</sup> NFC-enabled mobile payments have the potential to be the universal contactless payment technology if necessary stakeholders have the economic incentives to adopt it.

The slow evolution of contactless mobile payments in the U.S. is also indicative of a number of barriers that exist, as discussed in more detail later. As examples, the card networks, issuers, and acquirers have developed robust fraud analytics around mag-stripe technology and NACHA has developed monitoring processes which have mitigated ACH risk to a certain degree. Stakeholders are reluctant to invest in terminals and handsets in the absence of more certainty around changes to the infrastructure and the risk of making the wrong business decisions. The cost for merchants and issuers to invest in new device readers at the POS and for contactless chip-enabled payment devices, including cards, phones, and possibly other form factors, is significant.

Essentially, as discussed below, each primary stakeholder in the mobile payments ecosystem has its own ideas about how mobile payments should be developed and implemented, creating potential conflicts and barriers to development of a ubiquitous, interoperable solution for mobile payments. The market is moving quickly and there are still issues not fully resolved. So, there is benefit to convening the mobile stakeholders regularly to discuss the rules and framework of the mobile ecosystem as it evolves.

*Mobile network operators* (MNOs) own customer billing infrastructures that they can leverage to add value to existing voice and data services. While financial services such as mobile payments may represent an extension to existing customer relationships, the MNOs are new to financial services and have expressed concern about assuming material credit risk, based on their limited experience in providing consumer protections for financial services. However, the MNOs are experienced in providing subscriber acquisition and authentication, device provisioning, customer support and value added services, all necessary for increasing mobile payments. Additionally, they are a vital enabling technology channel for mobile payments.

*U.S. financial institutions* have not offered mobile financial payments because of a perceived lack of a good business case, although the growth in mobile banking implementations and recent mobile payment trials signal this may be changing. Financial institutions have the opportunity to add value to customer depository services with the addition of mobile technology and realize customer retention benefits as a result. With their long time experience handling payments, addressing customer authentication and authorization requirements, and enforcing Know Your Customer (KYC) rules,

---

<sup>9</sup> While there are other security options in addition to the secure element, e.g. cloud-based systems, this paper focuses on a secure element embedded in the phone.

financial institutions are well postured to settle payments to a consumer's account and to employ risk management programs that ensure regulatory compliance for money laundering, consumer protection, and other risks. Basically, financial institutions want to remain at the center of a customer's account relationship by issuing payment credentials and applications on the mobile device as they do in the physical payments world today.

*Handset manufacturers* must produce smart phones capable of including NFC technology and related security software and then pair with the MNOs to provide utility to the consumer. How to handle functionality around locked vs. unlocked phones, authentication, and the ability to use the mobile phone for NFC payments without the network all need to be addressed. Furthermore, technology needed on the handset to accommodate mobile payments is changing rapidly (e.g. SIM, micro SD, NFC sleeves) in order to address security challenges and compliance with MNO and payments certification. Yet, handset manufacturers around the world are beginning to issue standard handsets in volume that will embrace such technology in the next year or two.

*Trusted Service Managers (TSMs)*, building on their role in the card world, have emerged as the entity responsible for provisioning credentials to secure elements in mobile phones as a necessary tool to provide the type of transaction security users will accept. Depending on the size and scope of a TSM, other functions may include provisioning/account set-up; ensuring compliance with security requirements for software, hardware, handsets, chips and applications; fraud and risk management; and customer service and support. Customer support might include handling device/service questions and resolution relating to secure element use; developing and maintaining user documentation for best practices; support and assistance for operating system and mobile application software upgrades and mobile vendor certification; lost/stolen/updated phone notification to customers; handling billing questions; and reporting fraudulent transactions.

*Merchants* are critical stakeholders in the chicken and egg equation of mobile payments adoption. Merchants are interested in secure payments at the point of sale, timely settlement, manageable investment in infrastructure, relief from costly data protection inspection obligations, and reasonable interchange for transactions. Without widespread merchant acceptance, it will be difficult for NFC mobile payments at POS to achieve mass adoption.<sup>10 11</sup> Merchants must plan for and adopt the POS terminal technology necessary to work with wireless devices developed and deployed by the MNOs and handset makers. Depending on the application the merchant may need to interact with a particular bank. When the payments application used in a mobile transaction is a card application, the merchant must

<sup>10</sup> National Retail Federation. 2010. "Mobile Retailing Blueprint: A Comprehensive Guide for Navigating the Mobile Landscape," version 1.0.0. White paper, May.

<sup>11</sup> Merchant Advisory Group. 2010. "Open the Curtains in the Payment System - Merchant Advisory Group Recommendations on the Mobile Transformation Opportunity."

work with an acquiring bank to begin the clearing and settlement process. For ACH at the point-of-sale, the merchant must integrate with an originating FI.

*Intermediaries/third party processors and online payment service providers* have emerged to provide the enabling technology for mobile financial services or to serve as intermediaries in the payments supply chain. These processors and online payment service providers, mobile software solution vendors, and application and hardware developers are partnering with financial institutions or MNOs for the provision of mobile proximity payments. The third party non-banks see mobile as a new market opportunity and must be included in any infrastructure plans for mobile payments. They may also consider the existing environment too constrained by regulation and entrenched providers and seek to disrupt the payments ecosystem with a new offering.

*Consumer* demand for mobile technology is very high, but their interest in mobile payments is uncertain due to their lack of experience using mobile devices for that purpose. Consumers have many safe and efficient payment choices in the U.S. so the case for shifting to mobile payments must include new features and value. The rapid advance of electronic payments in the United States is a testament to the fact that ultimately, consumers want payments that are convenient, inexpensive, and secure.

*Payment Card and ACH Networks* all play a key role in the mobile payments ecosystem, although at this stage of the evolution, each network has chosen a different path to implementation. Some are partnering with mobile carriers to develop new ventures, while others are working with banks and transit authorities to test different or new forms of mobile wallets. NACHA is analyzing its rules to properly route new mobile payment transactions. Regardless of the interim actions, credit and debit card accounts will be critical to the long term success of ubiquitous mobile payments, given their dominant base of customers.

*Regulators must participate in the evolution of mobile* as the regulatory framework for mobile payments is fragmented with respect to MNO and other third party participation in the provision of payment services. In business model examples where payment flows leverage existing value chains of networks and payment clearing and settlement systems such as the card brands and the ACH, existing regulatory oversight and consumer protections are expected to prevail. However, questions are arising about the legal liabilities and responsibilities of new parties to the payments transaction, which may be governed by agreements between the stakeholders in the value chain. Participants desire clarity of the new regulatory structure and want to know how to be proactive in addressing consumer protection issues such as identity management, cyber-security and prepaid mobile accounts. Dialogue between FI regulators, the Federal Communications Commission (FCC), the Federal Trade Commission (FTC) and the Department of Commerce, *and* with mobile industry stakeholders is necessary to ensure that emerging

mobile payments services are conducted in a way that enhances safety and integrity in U.S. payment systems.

#### **IV. Long-Term Vision For the Future Environment**

As the MPIW discussed the future over a series of five meetings, a vision for the long-term mobile ecosystem emerged, in terms of successful business models and the important components of a mobile payments operating framework, such as standards and guidelines. While not all parties agreed in full, a decision was made to intentionally limit the scope of the effort to mobile payments at the point-of-sale. The group acknowledged that the mobile framework is not tied just to payments and that there is a need to look at opportunities to drive m-commerce, including value-added features such as coupons, rewards, clinical services, etc. The group further recognized that mobile has the potential to be a key component in making and/or securing remote payments and authenticating payments made via internet or card (i.e. card-not-present transactions). However, that possibility was viewed as something the group could discuss going forward.

The group opined that the potential societal benefits created by mobile-enabled payments technology, including the potential to reduce payments fraud and expand financial inclusion, portend a future where the mobile phone becomes the consumer's wallet and provides a seamless customer experience. This new mobile wallet will be enabled by NFC contactless technology embedded in the mobile handset so that it can store secure payment and identity information, as well as provide a secure access channel to payment services.

Ultimately, the successful mobile-enabled payments network will leverage a set of common standards and open platforms to ensure global interoperability. In a perfect world, mobile-enabled payments will be as interoperable as card payments are today, where consumers can use cards for payments anywhere in the world. Ubiquity will be achieved by creating a set of standards for payment applications that co-exist in a mobile wallet open to all card (credit, debit and prepaid) networks as well as ACH, that work across all carriers, and are accepted by all merchant POS terminals across all borders.

It is therefore critical for all participants in the future mobile payments environment to work together to design a model for interoperability that has the advantages of the card model and includes global industry standards. While the emergence of competing proprietary offerings encourages innovation, it also bears the risk of creating silos that may impede the development of critical mass needed to ensure a successful payments network. While workgroup participants were not in a position to establish consensus with respect to specific standards, all agree that the long-term vision of a successful mobile payments system in the United States will occur through the creation of mutually agreeable

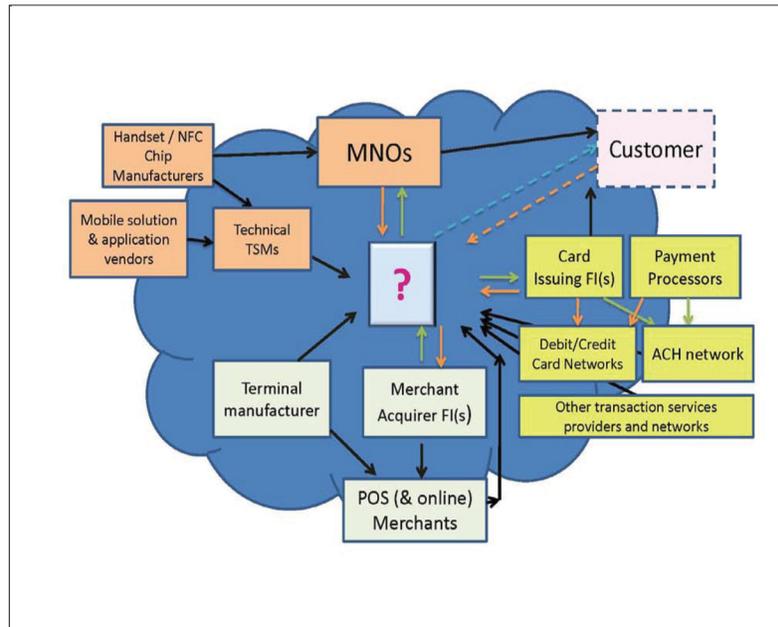
foundational principles. The goal of these principles will be to foster an interoperable mobile payments ecosystem; one that accommodates the customer of any financial institution or mobile carrier, thereby eliminating the need for compulsory customer movement between carrier or card brand (a common complaint today) and allows the customer to use multiple payment methods wherever merchants accept them. It is likely that a mutually agreed upon strategy will be necessary to provide the guidance and incentives to foster the evolution and migration to a ubiquitous mobile environment.

#### *Business models*

The major mobile stakeholders must determine the appropriate business model for the mobile payments infrastructure. The decision is complicated by the need to converge payments and mobile communications. The creation of a combined model requires the cooperation of multiple parties, including financial institutions, mobile operators, payment networks, technology service providers, chip and handset makers, and ultimately, merchants and consumers. While the MPIW did not discuss the different models at length, the consensus generally pointed to the possible co-existence of three basic business model scenarios within the mobile payments ecosystem (operator-centric, bank-centric and collaborative). In the operator-centric model the MNO owns the customer relationship for payments made using the mobile phone. In the bank-centric model banks own the customer relationship and mobile payments are processed over traditional payment networks (credit, debit or ACH). Each model could be utilized depending on the type and value of a purchase; the payment venue (e.g. physical POS, remote POS or internet); or other payment scenario.

The collaborative model (see Figure 1) emphasizes the need for an entity that would manage or work with all the parties in the mobile payment ecosystem to facilitate an efficient, holistic environment and provide oversight, business rules and standards for multiple service providers. This entity would serve as a neutral third party to assist other participants in creating a level playing field to facilitate faster and fuller market adoption. On behalf of all participants, it could tackle business issues of mutual need, such as determining the relative liabilities of each party, creating business standards and operating rules for handling customer problems, and leveraging the best practices and expertise of each individual mobile stakeholder.

Figure 1: Collaborative Model



The remainder of this section discusses how the different stakeholders might function with and without a collaborative framework in the mobile payments ecosystem.

**Mobile Network Operators**, working with partnered handset manufacturers, would continue to control access to the mobile channel and have secure elements configured into their offerings. However, they have limited experience with payment-related application or cryptographic data and while they have extensive account management experience, they have little experience dealing with banking and payment rules and regulations to protect consumers. Without collaboration of some sort, they would need to build new capabilities that go beyond their core business competencies to support mobile devices with broad mobile commerce capabilities; establish thousands of new relationships with financial account holders; and develop complex data centers that comply with industry security standards. Finally, MNOs would have to develop reciprocal agreements for commerce with each other so that account access could travel as easily from device to device as phone numbers do currently. In a collaborative model these elements could be managed by each party agreeing to a central set of guidelines.

**Payment Card Networks** have existing infrastructures for credit and debit contactless transactions and already perform a rules-making and fee-allocation capability related to card processing and

settlement. However, they lack access to the customer's DDA account and related data. Without collaboration they may not be able or willing to reach agreements about sharing data between competing entities.

**Financial Institutions** would continue to be at the center of their customers' financial activities, having a more trusted relationship and access to their own customer data, as well as secure data center capabilities that allow them to directly serve existing clients. Consequently, banks are well positioned to move consumers to new technology. However, banks will need the interoperability necessary to handle mobile payments involving other banks' customers and those customers who use different mobile carriers. Otherwise, without an open wallet, an FI would be able to work only with its own customers, unless it had bilateral agreements with other banks and carriers. Absent some scheme that facilitated multilateral relationships, having hundreds of bilateral agreements between banks and MNOs would be inefficient and fragmented, and not work well for mass adoption.<sup>12</sup>

**Payment Transaction Processors and Online Payment Service Providers** would continue to provide multiple-account payment processing services, perform credit and debit card provisioning and have existing extensive relationships with banks, merchants, credit card networks, pre-paid account service providers and technology providers. They would also have an extensive data support infrastructure to securely handle large amounts of financial and transactional data. While they might be able to provide more agnostic services for handling various credit and debit instruments, without collaboration they would need to establish multiple relationships with mobile carriers and expand relationships with banks to fully service consumer account management.

**Mobile Technology Solution Providers**, which include mobile payment application developers and TSMs, such as those who provision smartcards, secure elements and NFC chips, have the most experience and expertise with complex technology. While they may have collaborated on technical standards, such as ISO 14443, they have limited experience in dealing with payment rules and regulations to protect consumers. Technology providers would need to develop two-way relationships with carriers and banks, and with each other, since in some cases they are direct competitors.

A successful future mobile payments ecosystem requires an open payments system with interoperable services based on industry accepted formats, and technology standards that allow multiple parties to transact freely, but with some coordination and structure to ensure safety and efficiency within the mobile payments system. A collaborative model could provide stakeholders the opportunity to leverage their respective competencies for the collective good of the payments system overall. However, the number of stakeholders in the mobile ecosystem creates a more complex model that will require time

---

<sup>12</sup> For example, NACHA rules and ACH operator agreements create the effect of widespread multilateral agreements.

in which to establish industry norms for agreements and standards that will govern the interrelationships and their roles, responsibilities and liabilities. In addition, the MPIW was concerned that excessive coordination can sometimes stifle innovation.

Consequently, the MPIW felt that it was premature to consider such a model in the current market and it was decided to leave this discussion for a later time. Interestingly, a nascent version of the collaborative model was announced in November, 2010, by AT&T Mobility, T-Mobile US and Verizon Wireless, that includes a card network (Discover) and a bank issuer (Barclays Bank U.S.).<sup>13</sup> The joint venture, referred to as Isis™, is chartered to pilot a national mobile commerce network and an NFC mobile wallet. Isis will need to establish the rules of engagement, standards and customer needs within its collaborative effort and plans to have the scope and scale necessary to introduce mobile commerce on a broad basis, hoping to make it available to all interested merchants, banks and mobile carriers going forward.

#### V. Strategic Fundamentals of the Vision

The U.S. mobile payments market, particularly in the last year, has begun to move down what appears to be an obstacle filled path, absent any shared vision regarding key principles for success. All parties recognize at some level, however, that they share some common goals. Ideally, mobile commerce participants need to be able to flourish equally in the mobile ecosystem. FIs, merchants, payment networks and carriers need to be able to reach their own customers (and potential new customers) with innovative product offerings. Consumers should benefit from products and services that are standard and secure and that make purchase decisions easier for them, while a ubiquitous mobile commerce environment will provide the desired revenue opportunities. Further, through the implementation of common standards, costs can be reduced and integrity of the network increased.

As the MPIW met over the past year, the group's increasingly candid discussions led to a series of shared observations (or shared vision) about the nature of the necessary underpinnings of a successful

---

<sup>13</sup> On November 16, 2010, AT&T Mobility, T-Mobile USA and Verizon Wireless announced formation of a joint venture chartered with building Isis™, a national mobile commerce network to fundamentally transform how people shop, pay and save. With mobile payments at the core of their offering, they plan to create a mobile wallet that ultimately eliminates the need for consumers to carry cash, credit and debit cards, reward cards, coupons, tickets and transit passes. Isis expects to introduce its service in key geographic markets during the next 18 months. ATT, T-Mobile USA and Verizon Wireless collectively provide wireless services to more than 200 million consumers who will have access to the Isis service. Isis will utilize Discover's national payment network initially, which is currently accepted at over seven million merchant locations in the U.S., to develop an extensive mobile payment infrastructure for the joint venture, and Barclaycard US as the first issuer. See <http://www.paywithisis.com/#/news/>

future move to mobile NFC payments in the U.S. What follows is the workgroup's assessment of a set of foundational principles necessary to achieve mass adoption of NFC mobile payments in the U.S. These principles will require stakeholders to tightly coordinate efforts to develop a fully integrated end-to-end mobile payments process and represent a set of fundamental "business requirements" for success. The more rapidly they are achieved, the sooner the benefits of mobile payments will be realized.

#### *Foundation Principles*

##### *1. Open Mobile Wallet*

A successful model for the future should be based on a standard definition of an *open* mobile wallet, one that carries broad payment and merchant/marketing value options for consumer choice. Such a platform would embrace a technical architecture that enables the wallet to support a wide range of payment methods and networks, would comply with agreed upon industry business rules and standards, would employ a secure element or container in the mobile phone to interface with the mobile payment applications, and would utilize appropriate wallet protocols and processes, such as the ability for multiple payment applications to share the wallet. The mobile wallet would exhibit all of the flexibility resident in a physical wallet today, including payment-related functions such as loyalty program applications.

Current and planned contactless card/mobile NFC (pilot) deployments are not true mobile wallets by this definition as they offer constrained payment options which limit consumer choice and utility. Since the MPIW views mobile marketing, advertising and promotions, as well as transit, as primary business case drivers for NFC payment deployment (i.e., payment capabilities are a 'qualifying' factor in the business case, but not a 'differentiating' factor), there will be a need to understand and perhaps provide input on or recommend standards for security (including accommodating multiple payment options and applications with multiple secure elements in the handset chip accessing multiple regulated banking networks), privacy, compatibility and interoperability.

##### *2. Implement a mobile NFC contactless scheme with a specific (embedded) hardware component that may or may not include a micro SD form factor.*

The NFC scheme should be based on an industry standard, capable of supporting all payment methods and networks, able to comply with business rules and standards and reside in a secure container in the mobile phone to interface with mobile payment applications. The contactless NFC solution developed must work globally and in all venues (retail, transportation, as well as ATMs). Contactless payments employing computer chip security and near field communications (NFC or radio wave) technology based on ISO 14443 via mobile devices represent a preferred embodiment of future payments

in the U.S. When used at the POS, the contactless form factor should follow established contactless standards as endorsed by ISO and NFC industry groups, such as SmartCard Alliance, NFC Forum, Mobey Forum, etc. Who would be responsible for designing and developing the solution needs to be determined. Minimum compliance requirements for adoption should include dynamic data authentication, m-wallet contactless functionality and a secure element in the mobile phone.

Utilizing NFC contactless technology for mobile payments assumes that handset manufacturers will commit to putting NFC chips on a large number of new smart phones by some future date. It also assumes that the majority of merchant terminals in the U.S. will simultaneously be upgraded to contactless/NFC. Having some idea of when NFC mobile will be implemented, even without a formal roadmap, would help the merchants plan their investments. Achieving such synchronization, however, will require an extraordinary amount of collaboration, absent a highly participative forum for such discussions.

3. *Establish a ubiquitous platform for mobile payments that uses existing clearing and settlement channels and rails (credit, debit, ACH, prepaid, carrier billing) but allows for new rails as they are developed.*

The existing clearing and settlement rails are the necessary foundation for the mobile payments platform in order to create opportunities for mass adoption and consumer choice. While new payment channels may be created in the future, the MPIW supported the use of existing clearing and settlement systems to exchange payment information and value. Given the ubiquity of the ACH network, and the growing modes and ease of access to it, the ACH option may be critical for supporting a customer's desire to use mobile payments to replace physical cash or check transactions (i.e. non-card transaction) by enabling funds to change hands between parties via direct debit and credit. In addition, merchants who are too small (in sales volume and/or revenue) to qualify for accepting credit/debit cards could use ACH on the mobile phone to accept electronic payments in place of cash or checks.

4. *Adopt dynamic data authentication for long-term integrity and security in all card-based transactions and across all channels.*

Dynamic data authentication protects cardholder and other payments data by making each mobile payment transaction unique. A valid cryptogram is generated for each transaction, which is then verified when the transaction is authorized. The cryptographic value, including transaction-specific data elements, is validated through the terminal with the network to protect against fraud. The chip device (card or phone) must be present to generate a valid cryptogram, which is verified online or offline when the transaction is authorized. Many issuers already are providing contactless payment cards with dynamic

cryptograms, which is how contactless transactions have improved payment security. Dynamic authentication technology on mobile phones would lower fraud because, absent the sequential codes on the embedded chips, stolen payment card information could not be used to make counterfeit cards or fraudulent online transactions. In addition, the group noted the possibility that this technology could, over time, be applied to the card-not-present venue.

5. *Develop and adopt a global interoperable platform in the U.S. for standards and certification of payment methods for an open mobile wallet, applications, NFC, etc. Leverage existing standards where possible.<sup>14</sup>*

Using a special carrier-issued chip in the phone, consumers currently enjoy the ability to use their mobile phones on a global basis. Adding payment functionality to the phone, however, presents a number of challenges, particularly in the area of compatible standards. There are several existing mobile standards bodies such as GSMA, GlobalPlatform, ETSI (European Telecommunications Standards Institute) and the NFC Forum. Differences in what each standards body addresses and gaps in coverage for mobile payments will need to be identified and resolved, particularly where there is no overarching standard today, as is the case for a TSM in the U.S. Standards for implementing a secure element structure and technology must also be developed to ensure that a secure platform is open and works with multiple applications in the mobile wallet.

Absent a coordinating body, the industry will be hard pressed to analyze applicable global standards and the impacts to the different industry stakeholder groups, determine if changes to the standards are needed to accommodate contactless/NFC mobile payments and what the timeline and resource requirements would be. For the near-term (3-5 years) there is likely to be a wide array of initiatives to be aware of, provide input to, and consider incorporation of for deployment and operation in the U.S.

Full-NFC deployment will involve several infrastructure elements (e.g., a variety of secure elements in handset chips; multiple payment options with separate regulatory requirements in open wallets; management of security and operational services; etc.).

The industry will also need to consider how to address configurations other than full-NFC, such as micro SD cards or NFC stickers that perform lightweight implementations of NFC transacting. Some view these 'NFC-lite' deployments as preceding full-NFC in the U.S., and there are notable pilots involving banks underway and planned. Others view NFC-lite deployments as more likely to continue to occur after full-NFC attains critical-mass adoption, filling in with limited functionality, but sufficient security for users of less-advanced handsets, (i.e. backwards compatibility for awhile). The former view might relieve the industry from expending efforts that distract or dilute mapping out the infrastructure

---

<sup>14</sup> See Appendix IV for a discussion on current standards activities.

requirements for full-NFC, but the latter view raises the perennial need for the industry to figure out how to accommodate users who lag behind the technology adoption curve.

Finally, additional standards may need to be developed or modified to ensure that the NFC RFID chip communication does not interfere with other wireless network communication. The CTIA can potentially conduct tests to address this issue within its existing device certification initiatives; and improve clarity of member-driven initiatives for device certification. Working with CTIA members, terminal vendors, financial services providers and regulators, such as the FCC, the MPIW could assist in development of a comprehensive consumer, merchant and ecosystem-wide education and monitoring program.

#### 6. *Regulatory Clarity*

Mobile transacting will cross over domains covered by multiple regulatory agencies—the Fed/FDIC/OCC/NCUA for banks, the Department of Commerce for identity protection, the FCC for wireless carriers, and the FTC for consumer product protection.<sup>15</sup> The MPIW wants to understand sooner rather than later the regulatory focus and oversight regimen of each agency in the mobile payments world, as well as the applicability of current regulations and laws to the mobile environment, in order to avoid potential missteps as they proceed to develop mobile payments solutions. This was viewed by all parties in the MPIW as a key priority for the Fed to initiate and initial steps have been taken to begin dialogues with these agencies. A workgroup assigned to identify regulatory gaps, with supporting resources beyond the original MPIW membership, would assist in such an effort.

#### 7. *Trusted Service Managers should oversee the provision of shared security elements used in the mobile phone.*

There are several companies that manufacture secure elements. The TSM role would be to manage and control the provision of the secure elements in the mobile phones. The TSM may also perform other account management functions as discussed earlier.

Focusing on the core principles discussed above, the MPIW indicated a desire to continue meeting following a period of broader review of these principles by all stakeholders in the industry. The sense was, that absent any other inclusive industry forum, the continuation of the MPIW, perhaps in some expanded form, would benefit the stakeholders in the mobile ecosystem by providing a venue for the group to begin resolving some of the barriers and issues related to the list of foundational elements in order to successfully incorporate them into a mature system. For example, obstacles that need to be

<sup>15</sup>The new Consumer Finance Protection Bureau (CFPB) may ultimately weigh in on consumer protections for mobile payments.

resolved over the next 3-5 years to achieve true commercial adoption of NFC payments at retail POS may include commercial availability and widespread adoption of smart phones containing NFC chips; secure element resolution (ownership, standards, etc.) and implementation; identification and resolution of technical and business risk and security issues; agreement on the best business models; implementation of contactless readers at an acceptable number of merchant locations; agreement between regulatory agencies on regulatory requirements, assignment and changes (even if the regulatory changes have not yet been legislated); consumer and merchant education plans; etc. Many of these activities will likely need to be completed in overlapping periods, with some dependencies.

The MPIW also discussed the concept of developing an industry roadmap for moving forward, perhaps as a vehicle to clarify direction and encourage faster adoption of necessary change. Typically, such a roadmap might document a detailed explanation of the potential barriers to mobile payment adoption and recommend approaches (with cost/benefit analysis) to address them. A roadmap might also include best practices for the technology (hardware, software, terminals, chips); security (EMV<sup>16</sup> or something similar), dynamic data authentication, secure element (what is in the secure element and how is information involving payment credentials protected, etc.); interoperability; vendor/application management, vetting and certification; consumer relationship management (including enrollment, service and support for phone usage, recovery if lost or stolen, problems if bad applications downloaded); liabilities (who is responsible for exception handling and problem rectification); fraud and risk management practices to address consumer and merchant security; and regulatory protection and education.

In its fullest form, a roadmap could also discuss consumer use from an academic, non-competitive basis. It could identify the consumer value proposition, which is critical for achieving broad adoption. It could address ways to understand what motivates consumers and how to convince them of the benefits of switching payment methods. The roadmap could highlight ways to develop a viral marketing program to build mass adoption. Obtaining a better sense of consumer and merchant preferences and concerns would enhance the roadmap. In other industries, as well as payment associations such as NACHA, roadmaps are augmented by shared surveys directed at various stakeholders, which in this case would be consumers and merchants.

Ultimately, the workgroup felt that it would be premature to try to develop a roadmap that would influence the broad range of mobile payment stakeholders. The mobile payments industry is in its early stages of development in the U.S. and is characterized by experimentation and pilots which typically inform longer term thinking. Moving too early to determine common ground, establish standards, and

---

<sup>16</sup> EMV is used today in other countries for card payments. The MPIW discussed briefly the possible intersection of EMV with mobile payments in the U.S. For a more detailed discussion, see Appendix II.

develop rules of exchange could stifle innovation and reduce consumer choice. Further, certain key elements of the mobile payments infrastructure are still in pilot phase globally, implying that the adoption of standards (such as NFC standards) may, in some cases, still be a work in progress. In essence, the group felt that attention would be better focused on some selective barriers and issues in the short term and that an industry roadmap might better be approached in the longer term, if market forces produce inefficient outcomes.

Finally, the workgroup touched on another key issue - the role of the consumer helping to secure the future mobile environment. The group felt that future discussions should also include a plan to get consumer buy-in on shared responsibility for risk management. Unlike what unfolded with e-Commerce, where “zero liability” policies by the primary card brands produced a flood of repudiated transactions and so-called ‘friendly-fraud’ (along with a black market in stolen mag-stripe card credentials often fed by irresponsible cardholder behavior), the mobile venue needs to be *better*. That is, consumers need to buy-in to their role in ensuring a secure, private and efficient payments system and correct the bad habits they developed online. Consumer education related to security is critical for them to understand and know how to identify fraud risks on their end, assist in fraud prevention, and use the security tools that will be available to them in the mature mobile environment. Collaborating in some form to provide such education is a topic that needs to be addressed. Ultimately, the educational process must be coordinated, supported and, potentially enforced within the mobile ecosystem with a goal of helping consumers understand why they should upgrade to more secure handsets and employ best practices for usage in order to protect themselves and the entire mobile payments ecosystem from harm.

#### **VI. Potential benefits of contactless mobile payments ecosystem**

The creation of a contactless mobile payments infrastructure in the U.S. would provide a number of definable benefits, including improved fraud reduction capabilities, improved cost efficiencies for merchants and issuers, better data privacy, international compatibility, and reduced risk of settlement.

##### ***Fraud reduction***

The contactless mobile platform, replete with chip capabilities, can take advantage of the intelligence of the chip and the resultant layering of security tools to provide security features not present in today’s mag-stripe environment where skimming and counterfeit production are prevalent. The contactless mobile solution provides the framework for the enhanced security present in the EMV chip+PIN card environment, while also introducing new security layers unique to the mobile phone, including password protection to operate the mobile phone and access applications securely embedded in

the phone. Once at the mobile menu, access to individual mobile banking and payment applications can be further password protected. The EMV chip-based card, which can be replicated in the mobile chip, (although standards for contactless EMV must still be developed), contains individual account credentials, which can remain encrypted to the reader while an authorization is in progress (in some robust implementations). The PIN is also encrypted between the card and the reader, adding a second authentication factor dynamically to the transaction authorization.

Adding mobile data, such as location awareness, phone numbers or carrier accessed device IDs (e.g. MSISDNs or MDNs), can enhance account data, which banks use for risk management and the passing of encrypted tokens and PINs. Among cooperating stakeholders in the mobile ecosystem, utilizing all the data fields and information available with the mobile transaction end-to-end can logically and technically make the mobile transaction even more secure.

The mobile phone can also be used as a security tool for financial payments made at the physical POS and over the internet. The customer is always available, real-time, during a mobile payment transaction. If a network or issuer wished to authenticate customers with a real-time SMS challenge question, application or phone call, it could do so.

Furthermore, in addition to dynamic data for authentication, the mobile channel can support the other big fraud reduction initiative in the U.S.: preventing fraudulent transaction accounts from being set-up using credentials that might have been exposed (credit card numbers, demand deposit accounts, social security numbers, etc.). Better account set-up requires improved registration and enrollment processes, with higher levels of identity verification accessibility and utilization. The enrollment process for mobile banking and payments applications, including NFC provisioning and set-up with device-internal protections, could materially improve the registration and verification process. The additional enrollment process supplements the FI's own account-sign-up mechanisms and enables a much broader set of data about the enrollee to be collected.

It will be important to measure fraud reduction resulting from the use of a mobile phone vs. other payment methods to see how much mobile helped to reduce fraud. This may be difficult to do if companies are not willing to be transparent and share their fraud numbers and costs. Bank and other trade associations such as the ABA and AFP collect fraud data from surveys. The CTIA has a voluntary requirement for its members to complete an annual survey and report anonymously so perhaps they could help collect mobile fraud data through a survey.

With proper changes in regulations, this broader set of data has the potential to be shared within the mobile ecosystem. Full NFC implementations, augmented by encryption that works with the secure elements embedded in the phone, make superior payment account and user ID protections readily available. Ultimately, this benefit can result in both lower PCI compliance costs and lower fraud losses.

The MPIW can help maximize the opportunities for overall fraud reduction by working with the players to develop and implement fraud reduction standards for the entire environment that avoid the possibility of the network safety relying on the lowest common denominator. In addition, the group can work with the other parties to enforce standards and pursue bad actors

*Merchant cost efficiency*

The one-time cost of conversion to mobile payments may be viewed as a barrier (as described in the next section), but the ongoing and future benefits may be substantial. For example, mobile may provide an opportunity for merchants to reduce PCI inspection costs over time,<sup>17</sup> and reduce the costs and risks of storing sensitive data, as mag-stripe data exposure is eliminated. Short-term or one-time costs, including costs arising from merchant liability to issuers for accounts compromised from data breaches (in a mag-stripe/open-credential paradigm), are projected by some merchants to exceed the actual costs of fraud in the future if the industry stays with a mag-stripe standard. Many large merchants acting unilaterally are adamant about ensuring consumer payment choice, and appear to be prepared to support a number of alternative payment systems that take advantage of mobile and contactless capabilities. This includes advanced commitments and investments by merchants in chip+PIN for both offline and online transacting, which signals a growing understanding of the long-term business requirements.

*Lower issuer costs*

In the mobile payments environment, card issuance costs can be reduced by electronic downloads replacing expensive physical card distribution programs over the long-term. However, plastic cards are expected to co-exist with mobile phone payment options for several years, which will impact cost savings. And, current VISA and MasterCard rules require issuing of cards along with mobile accounts, so customers will carry cards and phones for a few more years. Costs to access TSMs and secure elements, uncertain at this time, must also be factored in. However, customer validation and activation can be simplified through more efficient, fully digital, and more secure (through the Global Platform standard) payment account provisioning, set-up and maintenance via the mobile channel. This would, in time, offset costs associated with phasing out mag-stripe cards. Loading cards to the mobile wallet will be less risky. Lost phones can be secured and remotely deactivated in ways that cards, wallets and purses cannot be, and there is evidence that consumers are much more attentive to the status of their phones. (Industry research states that it takes a consumer 4-8 hours to realize he lost his wallet, but only one hour to realize his phone is lost.) This can reduce fraud from lost payment accounts and make restoration of payment capabilities much faster and easier.

---

<sup>17</sup> See Visa Europe announcement at <http://usa.visa.com/download/merchants/bulletin-tjp-020911.pdf>.

*Data privacy*

The mobile channel can give a consumer the ability to opt-in or -out of applications and services offered by sellers and advertisers on a timely, case-by-case basis to control and limit access to private information. This requires the mobile channel to have effective and efficient regulatory check-points and roadmaps to ensure that the consumer has sufficient protections. Mobile can also have the broader benefit of triggering a proactive national agenda to drive toward consumer protections that lend themselves to individual preferences, versus universal blocks or hurdles that waste expense and effort to disable when circumstances warrant. Once again, standards developed collaboratively and orchestrated by a central party can enhance the data privacy process.

*International compatibility with a chip+PIN standard*

Implementing the international chip+PIN standard (or some yet to be defined alternative) generates additional benefits for the NFC mobile phone by making mobile transactions more fraud resistant. Ongoing mobile EMV pilots in Europe demonstrate continued evolution toward that end. Considering a near-term deployment of contactless chip+PIN mobile in the U.S. allows us to anticipate change and move in lock step with the rest of the world.

*Economies of scale and cross selling*

Mobile NFC technology is also being considered in non-payment and non-banking venues, such as transit and health care. As a result, investments in mobile payment technology may be shared over time, creating better economies of scale that will drive down the cost of future mobile solutions. The convenience and efficiency of the tap-and-go format can support many other applications that provide value-added services. Examples include high volume, high speed ticketing in transit venues; tap-and-go for parking meters, parking lots, and vending machines, and a variety of health care applications (e.g. making integrated, approved and authenticated purchases of medical products and services for insurance-defined accounts like Flexible Spending and Health Saving Accounts). Integrating rewards programs (from banks, merchants and third parties) can efficiently and effectively be orchestrated via mobile NFC wallets and applications as well—potentially increasing ROI for those programs.

*Consumer convenience, security and efficiency*

Surveys continue to show that consumers want to save time. Tap-and-go payment schemes can overcome the limitations and inefficiencies of 'self-checkout' and turn it into a sought-after mode of transacting, particularly when coupled with emerging shopping applications where the phone is used as a scanning device and barcode reader. Education programs can help consumers and small businesses understand that mobile technology has the potential to provide an even safer environment than exists today if implemented correctly. Consumers also want payment choice, and if possible, ways to consolidate all the cards in their physical wallets.

*Increased relevance of marketing, promotions and advertising*

The current one-way, one-size fits all broadcast-mode of buyer-seller interaction can be replaced with one-to-one, integrated communications and location-aware, real-time capabilities of mobile transacting. Services will need to be somewhat customized to reach different consumer demographics, since digitally oriented younger adults are more willing to opt-in to highly personalized services and commercial interactions, while older adults may avoid them. Recognizing that there are existing marketing regulations, use of the mobile channel for more extensive marketing may create gaps. Therefore, developing a regulatory roadmap will ensure that the industry invests wisely and appropriately to develop services that work in the interests of buyers and sellers without jeopardizing consumer protections. A properly guided mobile marketing, promotion, and advertising environment may create efficiencies and improvement in relevance, and convert wasted costs and investments into profitable new transaction streams that benefit participants in the mobile ecosystem.

**VII. Obstacles to Implementation<sup>18</sup>**

Despite the exciting business prospects and other benefits of transacting payments by mobile phone, there remains a significant amount of skepticism about how necessary, and how affordable, the transition to mobile NFC payments and, logically, their extension to EMV or similar standards, will actually be. The convergence of several major changes in the payments environment might finally be wearing down this traditional reluctance to change the status quo. Ironically, the unexpected attraction to mobile NFC increasingly appears to be the catalyst to finally moving from the mag-stripe paradigm to a payment system more fitting to today's digital economy and lifestyle. How and why this is happening makes a great study in consumer preferences and technology transformations.

At least four obstacles to implementation of a mobile NFC payment option with the breadth of impact thought by some to change the entire payments paradigm must be addressed and resolved:

- Cost of deployment
- Lack of adoption for contactless with cards
- Disruptive changes in the status quo for existing payments parties
- New revenue models and how to fund the changes necessary to create the mobile ecosystem

---

<sup>18</sup> See Appendix for Steve Mott's perspective of contrasting views on what motivates participants in the U.S. mobile payment ecosystem.

### **Cost of deployment**

The biggest obstacle to any transformation is the cost of the change. Upgrading the existing payments infrastructure from mag-stripe to smart cards and PINs has long been resisted by both FIs and merchants due to the apparent lack of a business case for the necessary investment. However, there is a growing sentiment that the conventional ‘wisdom’ about chip+PIN might have changed due to the need for global interoperability, as well as increased interest in moving to contactless payments on mobile phones.

One key factor about the lack of justification for shifting to chip+PIN might be the realization that the costs of PCI compliance (and clinging to mag-stripe) could soon exceed the costs of actual fraud. Ironically, merchants, who bear most of the costs of attempting to comply with these card credential protections, and who are increasingly exposed to financial liabilities to compensate issuers for mag-stripe fraud from data breaches, would pay more to avert mag-stripe fraud than issuers experience from the fraud itself. So, *any* substantive innovation in payments seems likely to devolve quickly from whether to replace mag-stripe to what technology to replace it with and how fast. Mobile NFC advocates make the case that their technology can facilitate this transition in a number of ways, and may prevent the need for a substantial build-out for chip+PIN contact cards in the process for the U.S.

Contactless advocates, including most big merchants, some of whom have already deployed terminal systems capable of supporting contactless chip+PIN technology, argue that the rest of the world is making steady progress moving to contactless. However, because of the overlap between the card world and mobile payments, some mobile stakeholders believe that it will be necessary to support both contact and contactless options in cards for some time, which if the market proceeds in that direction, will be more expensive.

### **Slow market adoption of contactless to-date**

Why should the U.S. also consider moving to NFC on mobile phones when the first generation of contactless has by some accounts been a disappointment?<sup>19</sup> Three reasons stand out for the apparent slowness in consumer adoption. First, consumers don’t really have an incentive to try or use contactless, vis-à-vis their other, familiar payment modes. With respect to more than half the cards issued, consumers aren’t aware they can *do* contactless. Additionally, it is difficult for consumers to figure out which merchants accept this format. Finally, banks have done little in the way of promotion, and have done a poor job of explaining to consumers that they will be *safer* with contactless.

---

<sup>19</sup> In the marketplace since 2004 with an estimated 70 million cards and fobs available for use in 150,000 merchant locations, but too few transactions to report so far.

The concept of mobile NFC is thought by many to address these constraints to consumer adoption by being fun to use, accessible to almost anyone with a mobile phone, and supportive (if the payment 'wallet' is open) of a multitude of payment choices, including prepaid for the un- or under-banked. Mobile devices can offer *added* security by providing more information to augment verification and integration of 'full' NFC, where the radio-wave chip and antenna enable the NFC application to interface with the secure element in the device's chipset. Two-way NFC capabilities may also offer another way for consumers to receive and redeem offers, promotions and coupons from merchants and third-parties—including many innovative exchanges based on location-awareness of mobile devices.<sup>20</sup>

The card networks primed the pump for merchant adoption of first-generation contactless payments, subsidizing the costs and deployment of several hundred thousand terminals, largely in the expectation that contactless would prove faster at checkout, cleaner to handle and therefore a good alternative to cash payments at the counter. But for the most part, the only payment options available are signature-based credit and/or debit, replacing cash transactions that typically cost less than a nickel to process with a signature-card transaction that costs \$.15 to \$.75 or more. This has not incented merchant support (such as prompting and assisting consumers to try the mechanism out). Additionally, merchants want to see equipment that looks the same and doesn't require retraining staff. Mobile stakeholders must work harder to identify a compelling need for merchants to accept contactless payments.

It is worth noting that as of February, 2011, industry estimates indicated there were 70 million contactless devices (mostly cards) and 150,000 contactless merchant terminals in the U.S. Despite the obstacles, this evolution of contactless cards at POS has been valuable, preparing and providing the industry with the experience needed to move to the next phase of contactless payments with mobile phones.

Merchants, from a variety of recent reports and publications, appear to have high expectations for the coming transformation in the payments environment. In particular, they are pushing for more payment choices with contactless, and pricing that better reflects the common view that mobile contactless—by virtue of being capable of greater safety and efficiency—should cost less than problem-prone mag-stripe payments. In the new consciousness of the raft of recent consumer-protection and merchant-assisting legislation, lower costs should be reflected in more advantageous pricing to merchants and lower purchase prices to consumers.

The NFC deployment configuration supports this new perspective by making an open payment wallet possible; even merchant-provided payment options (e.g., private label, store-card based, stored value) could be offered. That gives the consumer a full set of payment choices, and the possibility of enjoying automated rewards and loyalty benefits managed by the NFC/chip interaction.

---

<sup>20</sup>It is expected that offers, promotions, and coupons will also be distributed over mobile data channels.

The big inducement for merchants with mobile NFC contactless goes beyond the basic payment transaction. Two-way communications between the customer and the merchant enable more value-added innovations such as location-aware prompting to visit a store; identification of the consumer upon entering the store (to receive customized offers and promotions); facilitation of product promotions and coupon exchanges while shopping; and even a faster and more convenient self-checkout. And while it is fair to speculate that the mobile NFC version of contactless will engender much more merchant support, it is not possible at this time to estimate the revenue benefits associated with this concept.

Mobile NFC also enables the marketplace to bypass an aging, interim technology deployment (EMV contact cards) and focus investment resources on where the market appears to be headed in the future. This opportunity to save money and time should enable the new, mobile payments 'ecosystem' to build out a robust and efficient infrastructure that can benefit all parties.

#### **Ingrained Consumer and Merchant Payment Habits**

Perhaps the greatest barrier to change in the U.S. payments system over the past thirty years has been the consumer's comfort with the status quo. Check usage has just begun to decline over the past decade and even then at a reluctant pace. It took a decade to get consumers to utilize ATMs in meaningful numbers. POS systems were technically feasible in the early 1970s, but did not come into meaningful use for two decades. A significant number of beneficiaries still do not select direct deposit of government benefit payments and legislation may be required to achieve the last mile of change.

Merchants have understandably geared their changes to respond to consumer demand, not lead it. The cost of investments in new technology at the point-of-sale and the need to retrain staff to use new technology are clear deterrents to unnecessary change. These forces also tend to maintain the status quo.

Further, in the face of stiff competition, the banking industry has moved over the years to giving away most services (with the exception of credit carrying fees), offering them free of charge to the consumer; and focusing instead on charging for exceptions. Such practices have become a comfortable norm, making it difficult to use pricing as an incentive or disincentive to evoke change.

Finally, over the last fifty years, new payments options have been developed, but virtually no options have been eliminated. The consequence of this approach is inefficiency as a wide range of payment solutions continue to be supported, and even enhanced at the margin, despite apparent inefficiency.

Faced with these existing norms, consumers and businesses don't have a compelling need for changes in payment methods. Similarly, financial institutions faced with many competing investment opportunities in the wake of the economic crisis are not actively pushing change. As a result, progress in realizing a ubiquitous mobile payments ecosystem in the U.S. is likely to be relatively slow unless a

paradigm shift occurs in a key variable, such as fraud experience or regulatory change, or development of a truly new functionality that does not exist in current payment methods.

#### Revenue Uncertainties

Regulatory impacts are cutting away at many sources of card revenue and the market practices that make this revenue possible. Therefore, it is natural for the conventional payment industry providers to be concerned about the need to make incremental investments in a market in which timing of benefits is unknown, and about the uncertainty over whether they will be able to achieve the same position in the new payments paradigm that they had in the old, given the pressure on fees and the onslaught of new, non-bank competition.

Convergence of the wireless and banking sectors creates another perceived threat to revenue stability. It is assumed that both carriers and banks believe they own the mobile payments customer, provide the bulk of the value for mobile payments, and are attracted by the possibilities of increasing revenues related to transacting over phones. There is, at least, the potential for rivalries between the two powerful industries and many calls for cooperation in order to produce an efficient payment capability with fair compensation and return on investment for building out the necessary infrastructure.

Merchants, however, appear to be adamant about not wanting *two* big contenders in the payments 'food chain.' Instead, they point out that mobile payments ought to be safer and more efficient with the combination of both sources of data and network security from both industries, and that this lower risk and cost should be reflected in more attractive pricing *for the merchants*. Merchants propose a shift from the prevailing view that payment fees should constitute the financial foundation for a mobile transaction system, to a new perspective that payment capabilities might establish the *basis* for a new payment paradigm infrastructure, but not be the primary revenue model per se.<sup>21</sup>

Many of the participants in the old and the new payments ecosystem have expressed support for the development of a visionary infrastructure and a regulatory roadmap to help chart out what infrastructure, market practices and technology requirements can be expected and approved so that they can make the incremental investments needed that will be justified by viable business cases that are exposed to no surprises or undue risks.

Reaching such collaborative and enlightened cooperation will be a substantial challenge and might require a steady, sure hand from regulators from both the banking and the wireless industries to ensure an even playing field. Moreover, it is important to reach a quick consensus on what is required, and what

---

<sup>21</sup> National Retail Federation. 2011. "Mobile Retailing Blueprint: A Comprehensive Guide for Navigating the Mobile Landscape," January. The blueprint describes new ways for buyers and sellers to interact more efficiently and more gratifyingly with mobile NFC—setting the stage for revenue models based on mobile marketing, promotions, and advertising.

should be shared and non-competitive in the infrastructure, in order to develop and approve cross-industry standards to make certain the new, mobile digital payment system for the 21<sup>st</sup> century is even more reliable, ubiquitous, and robust than the one it will be replacing.

### **VIII. Conclusion**

This document is a work product stemming from the discussions of a Mobile Payments Industry Workgroup that was organized and convened by the payments research teams at the Federal Reserve Banks of Boston and Atlanta. While the ideas expressed in this document about a future success path for mobile payments in the U.S. are not directly attributable to any single member, they do represent a shared view of the participants about a way forward. Yet, even as the group met over a fifteen month period, many participants engaged in formative, independent partnership efforts to announce pilot initiatives to begin the exploration of mobile payments opportunities in this country. In many cases, the underlying concepts of these pilots are consistent with the vision expressed in Sections IV and V of this document; in other cases they are not. But, in all cases these independent efforts signal an appetite to pursue mobile payments as an important future strategy for payments efficiency, security, and convenience.

In essence, the concepts expressed in this paper represent a good entry point into the evolving mobile space that could create a more sustainable and efficient ecosystem through collaboration and sharing wherever possible. Group members ultimately thought that this could be a better way of doing business- agreeing early in the process on ways to build a highly ubiquitous and interoperable ecosystem model, while still competing fiercely on customer facing products and services. Moreover, by collaborating on key issues such as standards and rules of engagement, the sense was that the U.S. would be better positioned to be a part of a global mobile payments system that recognizes the flexibility and mobility of the phone as a payments instrument.

In other countries where mobile has emerged more rapidly, a central body from government, or one sponsored collectively by key private sector stakeholders, has helped organize and direct collaborative solutions. In some small way, the facilitating efforts of the two Reserve Banks noted above represents a microcosm of the benefits of having a central entity with no apparent "skin in the game" work with industry leaders to advance discussions. By providing administrative and thought leadership, the convening Reserve Banks were able to maintain a level of momentum that has resulted in this work product being developed in what, by industry standards, is a relatively short period of time. More importantly, though, the organizations that participated as members of this work group remained engaged throughout, while clearly expressing their independent views on very difficult key issues. Many of the

participants were meeting face to face for the first time and consequently the group went through a “getting to know you” period that eventually led to a willingness to share more openly for the benefit of a long term outcome desired by all. The need to establish a more enduring collaborative industry body is a decision that lies ahead, following a period of industry experimentation. Similarly, the benefits of establishing a cohesive industry roadmap for the future are yet to be determined, based upon the future identification of meaningful barriers to progress.

Ultimately, the value of this workgroup’s efforts will be measured by what happens next. Clearly, there are many more parties who will need to support the ideas set forth in this document, including the benefits of a central coordinating entity to work on behalf of all parties to create a roadmap for the future. Forums for engaging these parties may need to be established. This can only be achieved through broad circulation of the ideas in this paper and a decision by significant market leaders to foster further collaborative work. Existing industry trade groups and membership organizations will need to be an important part of this process. While there are notable precedents of success with such collaborative endeavors in the U.S. and overseas, there is also a long list of initiatives that ultimately failed because parties did not see the tradeoffs of independence and collaboration as beneficial. In many of these occasions, the underlying concepts never came to market or never achieved maturity because the obstacles to success could not be removed through independent efforts.

Yet, the opportunities and benefits of doing business differently with mobile payments in this country seem significant and the obstacles to success do seem daunting. Working together to pursue a common high level vision does appear to promise lesser investments over time by all parties and more rapid accrual of benefits than other options. Moreover, through enlightened collaboration, we all might benefit from the perceived view that if we get mobile payments right, it can be the entrée point to making other financial transaction services safer and more efficient. Beyond that, figuring out how to master fully flexible, digital and real-time transacting in payments and banking services might generate ways to bring more security and efficiency to other transactional domains, such as health care, government licensing, and even voting.

## **APPENDICES**

- I. Glossary of Mobile Terms**
- II. Cost of Converting to EMV in the U.S.**
- III. Elements of a Mobile Payments Business Case**
- IV. Mobile Payments Standards in the U.S.**

## APPENDIX I - Glossary of Mobile Terms

Term	Description
APRU (Average Revenue per User)	<ul style="list-style-type: none"> <li>Commonly used financial benchmark measuring the average monthly revenue per mobile subscriber</li> </ul>
CDMA (Code Division Multiple Access)	<ul style="list-style-type: none"> <li>Technology for digital transmission in which multiple frequencies are used simultaneously with each user having a unique code</li> <li>Each group of users has a shared code and only users associated with that code can understand each other</li> <li>Used to send voice, data, and signaling data (such as dialed telephone number) between mobile phones and cell sites</li> <li>Used in several countries including the U.S. and S. Korea</li> </ul>
Contactless Card/Device	<ul style="list-style-type: none"> <li>Use of either radio frequency (RF) or infrared technology to allow a payment card or mobile device and the POS terminal to communicate or transact without physical contact</li> <li>Contactless technology is popular with mass transit, road toll and physical security access applications which require fast transaction speeds.</li> <li>Consumer holds the contactless card, device or mobile phone in close proximity (2-4 inches) to the merchant POS terminal and the payment account information is communicated wirelessly via radio frequency (RF)</li> </ul>
Cryptogram	<ul style="list-style-type: none"> <li>A numeric value that is the result of data elements entered into an algorithm and then encrypted; commonly used to validate data integrity.</li> </ul>
DDA (Dynamic Data Authentication)	<ul style="list-style-type: none"> <li>Protects cardholder and other payments data by making each mobile payment transaction unique. A valid cryptogram is generated for each transaction, which is then verified when the transaction is authorized. The cryptographic value, including transaction-specific data elements, is validated through the terminal with the network to protect against fraud and skimming. The chip device (card or phone) must be present to generate a valid cryptogram, which is verified online or offline when the transaction is authorized.</li> </ul>
Downloadable Mobile	<ul style="list-style-type: none"> <li>Program residing on a mobile device</li> </ul>

Application	<ul style="list-style-type: none"> <li>• May be pre-installed by the MNO or handset manufacture but usually downloaded by the end-user, either via MNO or FI, or directly from the mobile phone store</li> </ul>
EMV – Europay, MasterCard, Visa Specifications (EMV)	<ul style="list-style-type: none"> <li>• Technical specifications and standards developed jointly by Europay International, MasterCard International and Visa International outlining the interaction between IC (integrated circuit) chip cards and terminals to ensure global interoperability</li> <li>• Standard for interoperation of IC (chip) cards and IC capable POS terminals and ATMs to authenticate credit and debit card payments</li> <li>• Purpose of EMV standard is to allow secure interoperation between EMV compliant IC cards and EMV compliant credit card payment terminals globally</li> <li>• EMV based credit card payment systems improve security (with associated fraud reduction), and the possibility for better control of ‘offline’ credit card transaction approvals</li> <li>• IC card systems based on EMV are known also as chip and pin</li> </ul>
GSM (Global System for Mobile Communication)	<ul style="list-style-type: none"> <li>• The most widely used digital standard for mobile or telephony</li> <li>• Open, digital cellular technology used to transmit mobile voice and data services</li> <li>• Has international roaming capability, allowing users to access the same services when travelling abroad as at home in over 210 countries</li> </ul>
ISO 7816	<ul style="list-style-type: none"> <li>• ISO standard for chip cards with contacts. The EMV standards are built on ISO 7816.</li> </ul>
ISO 14443	<ul style="list-style-type: none"> <li>• ISO standard for contactless chip cards</li> <li>• ISO 14443 defines two types of contactless standards: Type A (Philips Mifare) and Type B (Motorola)</li> <li>• Type C (Sony) is also widely used in Asia Pacific, but not yet formally adopted by ISO</li> </ul>
ISO 18092	<ul style="list-style-type: none"> <li>• ISO standard for NFC</li> </ul>
MMS (Multimedia Messaging Service)	<ul style="list-style-type: none"> <li>• Standard for mobile messaging systems that enables message to include multimedia objects such as images, audio, video, and rich text as well as plain text in SMS</li> </ul>
Mobile Banking	<ul style="list-style-type: none"> <li>• Access to bank information such as account balances and recent transactions via a mobile device</li> </ul>

	<ul style="list-style-type: none"> <li>Includes informational and transactional services, including bill pay, funds transfers, alerts</li> </ul>
Mobile Bill Pay	<ul style="list-style-type: none"> <li>Ability to set up and pay for various bills via a mobile device</li> <li>Mobile bills could be paid through mobile banking or through a third party or mobile operator</li> </ul>
Mobile Ecosystem	<ul style="list-style-type: none"> <li>A complex set of interconnected entities and relationships which interact to form a stable functioning payments system</li> <li>Ecosystem includes all payment system participants in the mobile payments environment, including financial institutions, money service providers, handset makers, technology service providers, mobile network operators, merchants and consumers, etc.</li> </ul>
Mobile Marketing	<ul style="list-style-type: none"> <li>Provision of advertising for mobile transaction services</li> </ul>
Mobile Payment	<ul style="list-style-type: none"> <li>Payment initiated from a mobile device. Mobile phone is involved in the initiation and/or confirmation of the payment</li> <li>Payer may or may not be 'mobile' or 'on the move'</li> <li>Mobile phone facilitates payment between the two entities in a C2B payment</li> </ul>
Mobile Parking (m-parking)	<ul style="list-style-type: none"> <li>Type of m-payment</li> <li>Ability to pay for car parking using a mobile device, typically via text messaging or possibly with a downloadable application</li> </ul>
Mobile Commerce	<ul style="list-style-type: none"> <li>Purchase of digital content such as ringtones and music, or physical goods in the same way a consumer would purchase over the internet</li> <li>Analogous to an e-commerce transaction</li> </ul>
Mobile Coupon	<ul style="list-style-type: none"> <li>Token, typically issued as a marketing or sales promotion, that can be redeemed at a participating physical or digital merchant</li> <li>Typically an incentive in the form of a discount on purchase goods</li> <li>Can be considered a subset of m-marketing, although the coupon itself may represent a cash value and may therefore be more directly transactional</li> </ul>
Mobile RDC	<ul style="list-style-type: none"> <li>Use of camera-equipped mobile phones for check image capture as a stand-alone application or as part of a broader mobile banking solution</li> </ul>

Mobile Remittances	<ul style="list-style-type: none"> <li>• P2P mobile transaction that crosses national borders</li> </ul>
Mobile P2P	<ul style="list-style-type: none"> <li>• Person-to-person mobile payments</li> <li>• Transfer of funds from one individual to another via a mobile device within the borders of a specific country</li> <li>• Uses SMS to send text messages with payment instructions to third parties, such as the bank accounts of customers, suppliers, or family members</li> <li>• P2P payments very popular in developing countries through service providers such as M-Pesa in Kenya and Smart Communications in the Philippines</li> </ul>
Mobile Ticketing	<ul style="list-style-type: none"> <li>• Ability to pay for , load and store mass transit tickets electronically on a mobile device</li> </ul>
Mobile Top-up	<ul style="list-style-type: none"> <li>• Transferring funds from a funding source (bank account, credit card, etc.) to top-up minutes on a prepaid mobile account</li> <li>• Minutes may be used as an equivalent for cash, allowing the mobile account to become a stored value 'wallet'</li> </ul>
Mobile Wallet	<ul style="list-style-type: none"> <li>• Software application loaded onto a mobile phone to manage payments made from the mobile phone</li> <li>• Can centrally and simultaneously store multiple applications managing customer account/transaction information with financial providers, public transit agencies, or third part entities such as health clubs, schools, and office or apartment buildings</li> <li>• Can also be used to hold and control a number of other applications (for example, payment and loyalty), in much the same way as a physical wallet holds a collection of physical cards</li> <li>• On-device storage technology allowing for the controlled and secure partitioning of information such as payment cards, coupons, mass transit tickets and medical information</li> </ul>
Mobile Web	<ul style="list-style-type: none"> <li>• Version of internet created to be accessed on mobile phones. Also know as mobile internet.</li> </ul>
MNO (Mobile Network Operator)	<ul style="list-style-type: none"> <li>• Also known as mobile carrier, the telecommunications business that provides mobile phone service to end-users</li> <li>• Has its own frequency allocation of the radio spectrum</li> <li>• Has the required infrastructure required to provide mobile phone service</li> </ul>
MVNO (Mobile Virtual Network Operator)	<ul style="list-style-type: none"> <li>• Business that provides mobile phone service but does not have its own frequency allocation of radio spectrum or all of the infrastructure required to provide mobile phone service</li> </ul>
Mobile originated SMS billing	<ul style="list-style-type: none"> <li>• Payment method via SMS where the payee originates the payment by sending an SMS text message to the customer</li> </ul>

Mobile terminated SMS billing	<ul style="list-style-type: none"> <li>• Payment method via SMS where the intended payee closes the payment by receiving one or more SMS messages</li> </ul>
NFC (Near Field Communications)	<ul style="list-style-type: none"> <li>• Wireless technology enabling communication between devices over a short distance</li> <li>• Used in mobile POS payments solutions</li> <li>• Short range, high frequency, standards based wireless communication technology which enables the exchange of data between devices in close proximity (less than two to four inches distance)</li> <li>• An extension of ISO 14443 RFID proximity-card standard that combines the interface of a smartcard and a reader into a single device</li> <li>• Communication occurs when two NFC-compatible devices are brought within four centimeters of one another</li> <li>• NFC can operate in one of two modes: passive or active</li> <li>• NFC contactless transactions clear over existing credit card or bank payment networks, not over wireless networks</li> <li>• Because transmission range is so short, NFC-enabled transactions are inherently secure</li> </ul>
NFC Sticker	<ul style="list-style-type: none"> <li>• A token containing RFID technology, allowing for the transfer of information between the token/sticker and the reciprocal contactless reader (e.g. mass transit access gate, contactless POS terminal, etc.)</li> </ul>
OTA (Over-the-air provisioning)	<ul style="list-style-type: none"> <li>• Transportation of messages wirelessly and without landline</li> <li>• Method of distributing new software updates to mobile phones or provisioning handsets with the necessary settings with which to access services such as MMS or WAP</li> </ul>
POS (Point of Sale)	<ul style="list-style-type: none"> <li>• Location where a transaction occurs, which is usually a retail store or similar venue, including public transportation, taxi cabs, restaurants, etc.</li> <li>• Equipment used by the merchant to complete the payment transaction</li> </ul>
Premium SMS	<ul style="list-style-type: none"> <li>• An SMS message for which the sender pays a higher fee than normal to cover the expenses for a good or service delivered</li> </ul>
Proximity mobile payment	<ul style="list-style-type: none"> <li>• Payment to a physical merchant that is initiated from an NFC-enabled mobile phone held in close proximity to the merchant's POS equipment</li> </ul>

Remote mobile payment	<ul style="list-style-type: none"> <li>• Payment initiated from a mobile phone to a recipient (person or device) where the recipient is not in the immediate area</li> </ul>
RFID (Radio Frequency Identification)	<ul style="list-style-type: none"> <li>• Automatic identification method that relies on storing and remotely retrieving data using devices call RFID tags or transponders</li> <li>• An RFID tag can be attached to or incorporated into an object to identify using radio waves</li> <li>• RFID tag contains an IC (integrated circuit) to store and process information and an antenna to receive and transmit the RF signal between devices (e.g. mobile device and a POS reader)</li> </ul>
SD Memory Card /micro SD chip	<ul style="list-style-type: none"> <li>• Secure digital memory card for removable memory in mobile devices</li> <li>• Used as a means of adding additional memory</li> <li>• Micro SD chip is a much smaller version of the SD memory card, which is now being used as a bridge to add contactless memory to mobile devices not equipped with means to interface with contactless POS terminals via RFIC and perform lightweight implementations of NFC transactions</li> </ul>
Secure Element	<ul style="list-style-type: none"> <li>• Platform where applications can be installed, personalized and managed, preferably over-the-air</li> <li>• Combination of hardware, software, interfaces and protocols that enable secure storage and use of credentials for payment, authentication and other services</li> <li>• Location of the security components, including confidential information, within the mobile phone</li> <li>• Location can be the SIM, a separate secure chip in the phone, or an external plug-in card</li> </ul>
Short code	<ul style="list-style-type: none"> <li>• Special shortened telephone numbers used mainly to address SMS and MMS messages from mobile phones</li> <li>• Widely used for such things as TV voting, ordering ringtones, charity donations, requesting product information, and mobile services such as SMS search services</li> <li>• Also known as short numbers or Common Short Codes (CSC)</li> </ul>
SIM (Subscriber Identity Module)	<ul style="list-style-type: none"> <li>• Removable smart card within a GSM mobile phone</li> <li>• Securely stores the service-subscriber key (mobile user account) used to identify a mobile phone to the network</li> <li>• Configured with information essential to authenticating a GSM mobile phone, allowing a phone to receive service whenever the phone is within coverage of a suitable network</li> <li>• SIM card allows users to change phones by removing the SIM card from one mobile phone and inserting it into another mobile</li> </ul>

	<p>phone</p> <ul style="list-style-type: none"> <li>• SIM card can be partitioned to store multiple forms of data</li> <li>• Can be used to host applications such as mobile banking applications</li> </ul>
SMS (Short Message Service)	<ul style="list-style-type: none"> <li>• Service for sending messages of up to 160 characters to mobile phones</li> <li>• Communications protocol allowing the interchange of short text messages between mobile phone devices</li> </ul>
TSM (Trusted Service Manager)	<ul style="list-style-type: none"> <li>• Neutral trusted third party intermediary or service provider that manages downloads of applications to mobile wallets</li> <li>• Securely distributes and manages contactless services for the application service providers' customers using the MNO networks</li> <li>• Provides a single integration point to all mobile operators for financial institutions, transit authorities and retailers that want to provide a payment, ticketing or loyalty application to their customers with NFC-enabled mobile phones</li> <li>• Owner/manager of the master key that controls the Secure Element platform. This allows the TSM to control and authorize service providers to install applications on the SE</li> <li>• Provides services to manage the secure download and life-cycle management of the mobile NFC applications for the FIs, transit authorities and retailers</li> <li>• Does not participate in any contactless transactions using NFC devices</li> <li>• Key functions include interconnecting with MNOs and application service providers; enrolling new customers; updating user interfaces; managing customer databases; managing application lifecycles; managing value-added service such as ticket reloading; and guaranteeing end-to-end security</li> </ul>
2D Barcode	<p>A 2D (two-dimensional) barcode is a graphical image that stores information both horizontally -- as one-dimensional bar codes do -- and vertically. As a result, 2D codes can store up to 7,089 characters, significantly more than the 20-character capacity of a one-dimensional barcode.</p> <p>2D barcodes enable fast data access and often used in conjunction with smart phones. The user photographs a 2D barcode with the camera on a phone equipped with a barcode reader. The reader interprets the encoded URL, which directs the browser to the relevant information on a Web site. This capability has made 2D barcodes useful for mobile marketing.</p>

UICC (Universal Integrated Circuit Card)	<ul style="list-style-type: none"> <li>• Chip card used in mobile terminals in GSM and UMTS networks</li> <li>• Ensures the integrity and security of all kinds of personal data</li> <li>• Typically holds a few hundred kilobytes</li> </ul>
UMTS (Universal Mobile Telecommunications System)	<ul style="list-style-type: none"> <li>• A third generation (3G) cell phone technology using CDMA as its underlying air interface</li> </ul>
USSD (Unstructured Supplementary Service Data)	<ul style="list-style-type: none"> <li>• Messaging technology unique to GSM phones</li> <li>• In contrast to SMS, which is a store-and-forward delivery system, USSD provides a continuous online session</li> <li>• Associated with a real-time or instant messaging type phone service</li> <li>• Response times are generally quicker than those used for SMS</li> <li>• It is a popular platform for mobile banking in South Africa</li> </ul>
WAP (Wireless Application Protocol)	<ul style="list-style-type: none"> <li>• Open international standard for applications that use wireless communication</li> <li>• Principal application is to enable access to the internet from a mobile device</li> </ul>
WAP Browser	<ul style="list-style-type: none"> <li>• Provides the basic services of a computer based web browser but simplified to operate within the limitations of the mobile phone</li> <li>• Program on mobile device that facilitates access to the mobile or 'real' internet from the mobile device</li> <li>• Commonly used web browser for small mobile devices such as cell phones.</li> </ul>

**APPENDIX II - Cost of Converting to EMV in the U.S.**

In 1998, the Tower Group conducted a detailed study of the cost of converting to EMV *contact* cards.<sup>22</sup> The total costs—most of which would have to occur at and with the POS systems—were calculated to be \$12.8 billion. That year, total bankcard fraud, as affecting the banks, was estimated to be less than \$1 billion—about a nickel per \$100. So it was difficult to make a business case on those numbers.

Yet the rest of the world was proceeding apace with planning deployment of EMV chip+PIN specs, which Europay (now a part of MasterCard), MasterCard, and Visa had developed and contributed as a global standard just a few years before. The specification provided for interoperability and synonymous security for encrypted chip card and PIN credit, debit and stored value payments.

Europe was experiencing much higher rates of fraud than the U.S. due to the lack of ubiquitous and cost-effective telecommunications infrastructure needed to conduct reliable and fast real-time authorizations. The U.S., on the other hand, enjoyed the world's best communications infrastructure. But there was still a lingering realization that eventually, if the rest of the world went to EMV chip+PIN, and the U.S. stayed with mag-stripe, payments fraud would migrate to the U.S., and U.S. travelers and merchants would be disadvantaged by not being able to transact with smart cards. At one point, Visa and MasterCard even proposed mandating the use of chip cards by 2005; that mandate never materialized.

By 2001, Tower Group re-checked its study on switchover costs to chip+PIN.<sup>23</sup> This time the total was \$13.4 billion. Merchant costs—adding in the need to accommodate the fast-growing online market—were projected to be three-fourths of the costs (bank authorization system upgrades accounted for 17% and bank network upgrades another 8%). Once again, there was no compelling business case.

Fast-forward to late 2009, when the Smart Card Alliance estimated total U.S. card fraud losses in 2007 at a still-modest \$1.7 billion, but indicated that total fraud was dramatically underreported, citing an estimate by the Mercator Advisory Group that adding in all merchant costs and the associated costs such as data breach forensics, lawsuits, undetected fraud, and misclassified issuer losses, the total cost might be more like \$16 billion, much of which was borne by merchants.<sup>24</sup> A Kansas City Federal Reserve paper, written by Rick Sullivan in 2010, estimated payment card fraud of about \$3.7 billion (using 2006 data), adding in the often unreported merchant costs!<sup>25</sup>

---

<sup>22</sup> Tower Group. 1998. "Smart Cards in the U.S.: An Infrastructure Cost Analysis," June.

<sup>23</sup> Iacobuzio, Theodore. 2001. "Smart Cards in the U.S.: An Infrastructure Cost Analysis (Redux)," Tower Group, February.

<sup>24</sup> SmartCard Alliance. 2009. "Fraud in the U.S. Payments Industry: Fraud Mitigation and Prevention Measures in Use and Chip Card Technology Impact on Fraud," October.

<sup>25</sup> Sullivan, Richard J. 2010. "The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options," Federal Reserve Bank of Kansas City, *Economic Review*, Second Quarter, pp. 101-132.

Importantly, the Alliance warned that retention of the mag-stripe on cards and POS readers would begin to dilute the fraud reduction benefits for countries that deployed EMV chip+PIN. Moreover, the growing dangers of data breaches, with big surges in compromised mag-stripe credentialed accounts, would inevitably require something other than a ‘do-nothing’ response.

In 2010, Javelin Strategy & Research echoed these concerns with their updated estimate of the cost of converting to chip-based contact cards (perhaps EMV, perhaps not) at \$8.6 billion.<sup>26</sup> One of the lingering deployment cost factors remains deployment of PIN-pads and terminals to cover the estimated 60-70% of retail, card-accepting locations that don’t have them yet. In the Javelin report, part of the motivation for moving to chip cards has now become the need for a true end-to-end encryption solution to data breach generated fraud and the growing costs and specter of PCI compliance. For example, by mid-2010, estimates to upgrade existing merchant locations that already process PIN-debit to comply with new PCI requirements might cost upwards of \$20,000 per store.

The most important argument for EMV contactless is that it could be materially cheaper to implement than contact cards. For example, in the convenience store industry, two-thirds of the outlets pump gas. The average store incurs an average of \$700 of card fraud per year. PCI compliance costs \$1600 annually—making that a stretch for business case justification all by itself. Outfitting the pumps with remote smart-card/PIN readers would cost an estimated \$50-60,000 per store/gas station.<sup>27</sup> With some 8% of retail sales in this retail vertical, EMV contact cards represent a huge hurdle. But contactless phones, communicating to inside the store via a Wi-Fi hotspot, could wind up costing less than \$5000 per store.

Some estimates suggest that EMV contactless could cost merchants as little as half the expense of deploying contact card readers (although banks and networks would likely experience little change in their conversion costs). However, to accommodate foreign travelers coming to the U.S. with EMV contact cards, a reasonable number of ATMs, travel venues, entertainment centers and food service facilities likely would need to accept the contact version, and U.S. issuers would still have to issue contact cards to U.S. travelers abroad.

---

<sup>26</sup> Javelin Strategy & Research. 2010. “End-to-end Encryption, Tokenization and EMV in the U.S.,” January.

<sup>27</sup> National Association of Convenience Stores estimate. 2010.

**APPENDIX III - Elements of a Mobile Payments Business Case, by Steve Mott<sup>28</sup>**

Changing the way people pay is difficult enough in any era, given the stability, predictability and fiercely preserved status quo the U.S. card payments system has achieved over the past half-century. By introducing technology (two-way NFC mobile handsets with chip-based security) that departs from the plastic card paradigm and can simultaneously become a catalyst for elimination of the magnetic-stripe infrastructure, the embryonic mobile ‘ecosystem’ discussed here is propelling an unprecedented disruption in business models—one that has old and new payments providers scrambling to come up with viable business cases.

The contention between old and new, legacy and future, and conventional versus value-added depicts the divergent interests of the mobile ecosystem as the participants jockey for position. Fundamentally, this is a \$300 billion industry<sup>29</sup> in which many established companies such as Visa, MasterCard, their big bank members, Amex, Discover, processors like First Data, Global Payments and TSYS, equipment manufacturers, and thousands of Independent Sales Organizations (ISOs), and many others (including consulting companies, law firms, and industry organizations) have profited substantially for decades.

New entrants, which include non-traditional payments companies with considerable presence such as PayPal, Intuit, Apple, and Google in addition to the giant wireless carriers (ATT, Verizon, T-Mobile and Sprint) and the handset manufacturers and application providers, are moving concertedly into the space with new technology innovations and business models. Consumers—especially smart phone users—appear to have put themselves up for grabs, constantly pushing and testing the borders of the walled garden of payments. And merchants, which have moved to the forefront of the discussion due to their singular role in deciding which of these innovations for mobile checkout at POS to embrace, are wielding unprecedented influence in both political and economic elements of this transformation.

Such robust participation suggests the dawning of a new ‘payments’ ecosystem, from which many more ‘parties’ will contend for portions of the emerging new revenue models for mobile transacting. If the new paradigm is chip-based contact cards, as many expect, the infrastructure replacement cost could easily be in the \$8-12 billion range—75% of which would logically be borne by merchants in terminal upgrades.<sup>30</sup>

One of the lingering deployment cost factors remains deployment of PIN-pads and terminals to cover the estimated 60-70% of retail, card-accepting locations that don’t have them yet. Online deployment of PINs is viewed as much easier, with most of the EFT networks and several of the big

---

<sup>28</sup> This section is adapted from a series of articles written by Steve Mott, Principal, BetterBuyDesign, 2009-2010.

<sup>29</sup> McKinsey & Co. 2009. “Payments Industry Roadmap.”

<sup>30</sup> Javelin Strategy & Research, 2010.

processors now adopting software-encrypted PIN-debit capabilities. No additional infrastructure is needed by consumers, merchants or issuers in order to process these transactions over the internet.

Perhaps for the first time in this country's conversion to electronic payments, the sustaining business case appears unlikely to be made principally on garnering new transaction fees or reducing payment processing costs. Rather, it will likely be made by wholly different cost avoidance and revenue drivers altogether. And several external influences are converging to suggest that the new ecosystem will be driven far more by new revenue drivers than 'tolls' for doing payments.

What follows is a general discussion of the elements to a business case, as well as an assessment of the potentially important business case ingredients for the major players in the ecosystem. At this time, it is very difficult to place meaningful estimates on the potential value of each business case element. This will become more possible over time as various pilots are performed, new regulations are finalized, and new technology is unveiled. However, it is important to recognize that the factors discussed below be evaluated as part of a holistic business case assessment both by individual firms and, perhaps, by industry overseers as part of an effort to understand any public policy issues that may emerge. It is also important to note that while few have demonstrated a clear business case for the full adoption of a mobile NFC payment infrastructure in the U.S. to date, the vast range of announced pilots are evidence of widespread interest and anecdotally, many key players are sensing that the time is near.

#### **External Influences on the Business Case**

There are a number of disruptive changes occurring in the world of payments today that are upsetting the status quo, and continuing to push conversations about new payments technology, such as incorporation of mobile phone payments, to the over-arching issue of the need to overhaul/replace the existing mag-stripe infrastructure:

##### 1. Security issues with mag-stripe/stolen credentials

Funding terrorist operations with stolen credit card and debit card credentials—which can be easily obtained from hundreds of black market websites for often less than a dollar—raises questions about how long the U.S. can persist in supporting current mag-stripe technology, when chip-based security for credentials is the standard for every other developed country in the world.

*NFC payments, using a contactless chip in the handset that houses secure elements that protect account credentials, and communicates them securely through the NFC chip and antenna to the terminal, represents a new payments paradigm. Current and future cost avoidance opportunities and future reputational risk costs stemming from a move from mag-stripe to a mobile*

*based NFC world should become part of any business case analysis. Data associated with this move can be gleaned from current and proposed initiatives in other countries.*

## 2. PCI compliance requirements and costs

Recent merchant association estimates (most recently from a survey by the Merchant Advisory Group in October 2010) project the amount of money merchants have spent to-date on trying to comply with PCI data protection requirements to be \$20 billion or more, with annual costs expected to exceed \$2.5 billion by 2014—more than the reported bank cost of payment card fraud itself. If accurate, such an investment would have easily paid for conversion to chip and pin technology. Merchants are uncharacteristically motivated to abandon the mag-stripe paradigm in order to rid themselves of this burden alone.

*NFC payments securing account credentials from the handset chip to issuer authentication in a widespread deployment has the potential to greatly reduce merchant PCI issues. Those aspects of PCI compliance that can be satisfied by a robust mobile implementation should be factored into a business case assessment.*

## 3. Endemic Fraud

Most payment card fraud containment activities in the past five years have related to PCI compliance, rather than attacking the sources of fraud,<sup>31</sup> leaving the industry with an ambient issuer fraud rate about \$.05 on \$100 in spend. That means absolute fraud losses continue to grow with volume, and if merchant and third party fraud losses are counted in the conventional estimate of about \$2 billion in ambient card fraud (U.S. issuers only), future fraud losses could be 5-10 times that amount with all parties' losses counted in.

*It is getting more difficult to justify continued investments in tweaking the mag-stripe infrastructure—versus investing in stronger, more digitally capable technologies—such as full NFC payments using secure elements and electronic wallet functionality. Future estimates of growth in fraud losses need to be a part of the business case, as opposed to historic costs<sup>32</sup>.*

## 4. Exported fraud

---

<sup>31</sup> VISA submission to the Federal Reserve in anticipation of the proposed rulemakings regarding the Durbin Amendment to the Dodd-Frank Financial Reform Act, fall, 2010.

<sup>32</sup> In late 2009, when the Smart Card Alliance estimated 2007 total U.S. card issuer fraud losses at about \$1.7 billion, but indicated that total fraud was dramatically underreported, citing an estimate by Mercator that adding in all merchant and associated costs such as data breach forensics, lawsuits, undetected fraud, and misclassified issuer losses, the total cost was closer to \$16 billion --much of which was borne by merchants.

By clinging to mag-stripe, the U.S. also forces overseas deployers of chip+PIN cards to retain the mag-stripe on the cards they issue so that their customers can use them when in this country. Similarly, merchants overseas must prolong use of mag-stripe terminals to accept cards from U.S. customers. In effect, the U.S. is 'exporting' fraud to overseas issuers and merchants; yet few U.S. issuers are converting to EMV so far, and Visa and MasterCard are still non-committal on how fast they might support a conversion to EMV.

*EMVCO has completed its initial contactless specification but needs to ensure that it conforms to generic use and interoperability, while Visa and MasterCard state their conversion plans and aim for the same kind of compatibility.*

5. Regulatory impacts on signature-based card rates and pricing practices

The Durbin Amendment to the Dodd-Frank Financial Reform Act could result in outcomes that reshape debit card economics and competitive practices. For example, some suggest that in aggregate, the prospects for continued use of signature debit will dim in favor of PIN-debit. An estimated cut of 75% of interchange rates, to a cap of \$.12 per transaction, may challenge existing business models for alternative payments in place today. Also, the current regulatory impetus seeks more competitive debit network access choices for consumers and merchants.

*In open wallet configurations, where multiple payment types and networks can be accommodated, NFC payments can satisfy emerging requirements for broader payment choice. Final regulations on interchange and options will create a new business case environment for some of the critical parties that may carry over to the mobile environment.*

6. Technology shift in consumer behavior

A persistent move is underway to on-the-go, real-time, mobile transacting as part of a versatile digital lifestyle for the young, including a new cohort of mobile bankers. Downloading of applications on increasingly sophisticated smart phones, coupled with the opening up of payment networks (e.g., PayPal, Visa, Intuit, MasterCard, etc.) for applications development, portends unprecedented opening of access for payment transactions. Mobile handsets have begun replacing wallets and pocketbooks with younger and tech-savvy consumers, and offering break-through utility and innovations in lifestyle.

*While NFC-'lite' architectures (e.g., micro SD) may satisfy some of the utility of these innovations today, there is growing evidence of a concerted move to full, two-way NFC-enabled handsets—which will both accommodate digital lifestyle enhancing applications and support the commercial innovations discussed below. Use of mobile NFC solutions in symbiotic non-payments*

areas will have an “improved economy of scale” effect on payments applications that could bring about improved unit costs.

7. Technology cost improvements.

In growing technology markets, prices characteristically improve over time as sales volume grows and standards are adopted. Because of the state of the mobile evolution in Europe and elsewhere, NFC standards are emerging and terminal manufacturers are deploying systems that already contain elements to support various types of non-mag-stripe card offerings, as well as mobile NFC. In fact, some U.S. merchants have already deployed such capture devices, while others have such plans, and still others are positioned to add on new technology.

*This implies that the business case for merchants may not be as daunting as predicted in the whole. If so, the chicken and egg problem of customer demand and ecosystem ubiquity may diminish.*

8. Improved buyer-seller interactions at POS

A slower growing economy overall, with little opportunity to raise prices when so many consumers (and businesses) are struggling financially, has propelled merchants to pursue new business models that improve on the poor historical results they have experienced with ‘broadcast-mode’ advertising, marketing and promotions, such as free standing coupon inserts in newspapers or store circulars. Instead, they are determined to use mobile technology to influence new customers to sample their stores, spend once they get in stores, try products the merchants (and manufacturers) are pushing, and exchange information that helps attract, grow and retain the relationship over time.

*Two-way NFC enables real-time, location-aware interactions that combine shopper behavior and history with tailored, one-to-one promotions and integrated loyalty programs. As a result, some merchant groups are advocating a concerted move to contactless technology—bypassing the costs of deploying contact cards where possible. Moreover, the merchant business case for mobile is significantly enriched, if not substantially justified, by the marketing opportunities resident in mobile payment alternatives.*

These influences taken together will shape which business models will survive or get traction in the decade ahead for the key participants in the evolving mobile payments ecosystem. In particular, if the U.S. payments market is indeed beginning to migrate to chip secured account credentials and PIN verification of cards at merchant terminals/network interconnections (whether based on the EMV standard

or something perhaps better), there will be many doubts about what interim technologies to invest in until or unless a new payment paradigm takes hold.

But there are fundamental conflicts that exist at the level of basic business interests of many participants in the new ecosystem that further complicate the decision on whether and to what extent to cooperate in a symbiotic sharing of new, non-competitive infrastructure. The differences in the business case pros and cons for the major participants are themselves revealing of the complexities inherent in transitioning a previously isolated business model to a more holistic one that can support the need to scale to huge volumes, provide security in ubiquitous retail environments, and interoperate in a seamless and transparent fashion. Replicating those attributes will be a daunting task.

#### *Conventional Payments Stakeholder Business Challenges*

Starting with the existing, conventional payment card transaction providers—banks, bankcard associations/networks, processors, and terminal providers—for whom the status quo—recent regulatory changes in interchange and banking fees notwithstanding—has produced a sustaining and substantive business opportunity, participating in the emerging mobile ecosystem presents unusual business case challenges.

##### *Banks*

Twenty years ago, banks depended primarily on interest rate arbitrage for the bulk of their earnings. Today, more than two-thirds (cite?) of bank revenues come from an assortment of fees, charges, and other pricing for services. Tomorrow, banks will earn billions less from consumer fees and pricing (e.g., on checking account overdrafts), and an estimated 75% reduction of interchange revenue on debit cards. Pressures are expected to mount to lower merchant costs for credit cards as well. For the top 10 banks, which control over 90% of credit card revenues, and get 20-30% of overall payment revenues from credit cards, the economics of the signature-based payment cards status quo is declining dramatically. So a lot is riding on making sure that bankcard payment options make it into new venues like mobile.

Implementing EMV contactless could be materially cheaper to implement than contact cards in some retail sectors that have resisted any wholesale change at POS. For example, in the convenience store industry, two-thirds of the outlets pump gas. The average store incurs an average of \$700 of card fraud per year. PCI compliance costs them \$1600—making that a stretch for business case justification all by itself. Outfitting pumps with remote smart-card/PIN readers would cost an estimated \$50-60,000 per station (according to the National Association of Convenience Stores). With some 8% of retail sales in this retail vertical, EMV contact cards represent a huge hurdle. But contactless phones able to communicate into the store via a Wi-Fi hotspot could cost less than \$5000 per store.

The banks, and their card payment associations, argue that they already provide consumer access through hundreds of millions of existing payment accounts, and merchant acceptance at 8 million locations. Moreover, they have global networks that already scale to huge volumes and generations of risk management experience. So the business case for their participation in mobile NFC payments is: ‘use what’s already there’ and adapt the existing infrastructure to evolving needs. The question, of course, is at what level of economics for what participants? And whether they will manage a chip+PIN paradigm with more flexibility and balancing of compensation than exists with the mag-stripe model.

Bigger banks experience an intensity of reactions from these influences, owing to both the considerable money they have historically made on signature-based, mag-stripe cards—at least until the coming year—and the investments made in both online and mobile banking and card use. Smaller FIs face a quandary of their own, contrasting a keen and growing desire to be relevant to the digital savvy, under-35 cohort of financial services customers, and the need to find a way to obtain infrastructure services to allow them to do mobile banking, mobile payments, mobile marketing, and—prospectively—chip and pin. Those are daunting choices and investments to make at a time in which industry wide debit card revenues might drop by \$15 billion or more.

#### *Payment Networks*

While fundamentally aligned with their bigger banking members, Visa and MasterCard as public companies are increasingly driven by the mandate to drive more transactions across their networks—even if they come from non-banks/non-members. Step-by-step, these publicly traded payment networks have pushed into prepaid, contactless, P2P payments and more recently, versions of NFC-based payments, doing pilots with both bank members and non-banks. And, they are not as impacted financially by the regulatory changes sweeping the current payment card business. So, it is logical to expect them to be at the table for any consideration of mobile payments infrastructure and business opportunities.

What is not so certain is the business case for the ecosystem’s use of their networks, and ascribing to their network rules and requirements. After decades of exerting material influence over industry pricing, the mobile payments paradigm in the new regulatory environment appears to be seeking different revenue models going forward—particularly those where the mobile handset interaction in merchant locations fosters real-time, location- and customer-aware decisions on purchases, and where big and powerful non-banks (e.g., wireless carriers) are key players.

Closed-loop charge card companies like American Express and Discover stand to play intermediary roles in architecting new variations of mobile payments, as recent market initiatives indicate. Because they have nearly the same merchant acceptance ‘pipes’ as the credit card payment networks, and can offer national access for tens of millions of consumers with their payment cards, they can be a factor in any new business calculation. For them, the business case is new transaction volumes from potentially new

customers who utilize them for mobile applications, with merchants still willing to pay prevalent credit card transaction fees.

Non-profit payment networks such as the ACH network and other PIN debit networks also provide payment utilities for their financial institution members of all sizes. Volume is also important to these networks as they develop rules to balance the appropriate amount of innovation with risk management for the benefit of their FI members, which enable valuable solutions for their clients.

#### *Processors*

Payment card processors are a lynchpin to the existing infrastructure, but will be called upon to make major changes to their network configurations—particularly to accommodate passing encrypted account credentials through their terminals and networks straight through to chip and pin implementing issuers. This is not a trivial task. For example, in order to minimize the deployment changes required in processor environments overseas when EMV was implemented, Visa and MasterCard have temporarily permitted use of static authentication of chip card transactions (rather than dynamically generating unique data) and decrypting the account credentials at the merchant terminal so they could pass through the processor network to the issuers. Similarly, processors were given two-and-a-half years longer to become PCI compliant than their big merchants were, meeting these requirements only by mid-year 2010 as mandates.

Like the payment card associations, the key economic driver is the *volume* of the transactions, versus the interchange fee rate. So as long as processors can derive a business case for making the infrastructure changes, they would be largely indifferent as to what type of payment was being generated. Moreover the liability shift that accompanies robust implementation of chip and pin would largely make processors' lives easier, and perhaps lower cost due to the reduction in charge-back and other exception handling costs.

But, with some exceptions, many processors have remained silent on the much-discussed mobile 'transformation', and have focused on preserving the funding levels that the payment card industry has historically generated, for as long as possible. That is perhaps understandable in a part of the business that has borne the brunt of price compression from both merchant discount fees and the associations' pass-through of acquirer fees for many years. Their clear concern: how many of which alternative payment types and technologies must they tool-up to support?

#### *Terminal Manufacturers*

For several years now, higher end POS terminals have spawned a rich array of functionality to support PIN-debit, prepaid, ACH, barcode, and even biometrically authenticated applications. A standard terminal now contains hundreds of potential applications that need only simple downloads or on-site programming to activate. Such application-migration now extends to EMV contact card reading

capabilities, as well as vanilla contactless tap-and-go radio signaling. Attaching a full-NFC reader to these terminals is fairly straightforward, and can cost about \$300. Some recent quotes for both EMV contact card and contactless combination readers are around \$400 per terminal, if deployed together. For these participants of the ecosystem, change is usually a good (and profitable) occurrence.

Such forward-thinking infrastructure planning has been embraced by some of the nation's biggest merchants. For example, Wal-Mart, BestBuy and HomeDepot—among others—are currently able to accept EMV contact cards around the world, and Wal-Mart has publicly predicted EMV transactions in the near-term (BestBuy and HomeDepot were also early adopters of contactless tap-and-go). Meanwhile, hundreds of smaller merchants in U.S. states along the Canadian border are already accepting EMV card payments from their foreign shoppers using cards issued by Canadian banks.

The sticky problem with terminals, however, is the business case for getting the millions of smaller merchants to upgrade their terminals. For example, there are roughly 400,000 merchants still using Verifone Tranz330 terminals which were first introduced in the mid-1990s. These terminals have limited applications for largely mag-stripe only transactions, and subject the system to much inefficiency—like the ability to commit rudimentary fraud (e.g., with forced draft capture). Many of these merchants are likely to protest even POS upgrades that cost them only a few hundred dollars—just as they have resisted PIN-debit pads over the years, even though the additional monthly cost is typically less than a dollar.

#### *Merchant Requirements*

A primary but until recently reticent player in any payment ecosystem is the merchant base. Perhaps emboldened by a recent surge of support from Congress, regulatory agencies and the courts and with an unusual sense of unanimity, U.S. retailers have largely embraced the mobile transformation—partly as a way forward from a payments business model largely unchanged over decades, but mostly as an opportunity to gain one-to-one relationship connections with customers, and truly drive incremental, competitive sales.

To that end the National Retail Federation introduced a report in mid-2010 (updated in January 2011) called the *Mobile Retailing Blueprint*, containing an extensive list of innovations that NFC-enabled and other mobile payments could bring to the retail sector.<sup>33</sup> At the end of 2010 the Merchant Advisory Group published a set of policy and infrastructure recommendations to put their spin on what should be done implement the Blueprint as soon as possible.<sup>34</sup> Among the suggestions: focus deployment on EMV contactless, bypassing EMV contact card deployment where possible, to avoid transitional investments in technologies that will not be essential in the future.

---

<sup>33</sup> National Retail Federation. 2011.

<sup>34</sup> Merchant Advisory Group. 2010.

Most importantly, though, the merchants active in contactless and NFC mobile payments implementation seek an ‘open wallet’ configuration, where consumers can load as many payment choices as they want, and merchants can search for the payment options they prefer in the transaction session. Such choices would include standard credit and debit account options, but would not be restricted—as they are today for the most part—from doing PIN-debit, prepaid, merchant private label, or even ACH transactions. Transactions from third parties—PayPal, BlingNation, Obopay, Western Union—could co-exist with those from the traditional payment brands. There is even talk of cross-merchant acceptance of closed-loop, private label, merchant-provided credit and prepaid options

Such new requirements from such an important part of the mobile payment ecosystem foretell a much more competitive environment for transacting than has ever existed before, and makes the notion that both banks and carriers could build their business cases mainly on joint assessments of payment fees a much less likely route for tomorrow’s revenue model. In other words, the business case for NFC payments must go beyond the payments component.

#### *Other Ecosystem Participants*

New participants in the mobile payment ecosystem (e.g. wireless carriers, application providers/markets, handset makers, security providers, system integrators, trusted service managers, etc.) all have their own revenue and profitability objectives. Until very recently, they expected some portion of payment fees to drive the business case for their participation. While much of the arms-length jockeying between banks and carriers for ecosystem support over the past two to three years concerned which industry would charge the fees (to merchants) and how those fees might be divided up, the recent merchant ‘activism’ (and apparent exploration of market alternatives) has changed the nature of the ‘conversation’ toward who provides what value, and what is fair compensation for that value.

#### *Wireless Carriers*

Three of the big carriers announced a joint NFC initiative (called Isis) in conjunction with Discover and BarclaysCard in November 2010. Details were sparse, but the idea was that the built-in NFC wallet would be restricted to carrier-specified payments, and the carriers—rather than banks—would earn the interchange portion of merchant fees. Several reports on Isis concluded that besides aversion to any restrictions on payment choice, some merchants were disappointed that a new revenue model that improved on the interchange convention had not materialized.

If nothing else, this announcement put the payments world on notice that some big players with deep pockets wanted to participate. The carriers’ ability to package and bundle services built around heavily marketed handsets demonstrates their ability to steer consumers to more and more advanced services. Whatever the fate of Isis might prove to be, carriers appear likely to be important for the front-

end outreach necessary to spur consumer adoption. Moreover, Isis fueled consideration that, while carriers were clearly seeking new sources of stable revenue for a wireless business that underwent constant price compression, the other assets they brought to the mobile table were very important to factor in to the ultimate business case. Certainly their ability to operate huge networks undergoing rapid change, and their ability to incorporate relentlessly evolving technology with persistent risk management challenges made them a worthy partner for mobile commerce.

The biggest revelation was the possibility that carriers, who collect unique handset identification numbers, the cell phone number associated with a registered account, a location over a specific network, and other verifying data, could become valuable fraud mitigation partners with banks, which know a purchaser's registered account number, associated authenticating information, bank account history and behavior, and usage patterns. In combination, mobile payments could be materially safer than any other payment mechanism, and the properties of end-to-end digital transmission and authentication points could make mobile payments more efficient as well. Regardless of all the above motivations, carriers stand to handle and charge for more traffic across their networks than experienced in traditional non-mobile payments systems.

#### *Application Providers/Marketers*

Any observer of the explosive phenomenon of Apple iPhones and their cavalcade of applications (including dozens of payment utilities for both consumers and merchants) can see where the mobile payments market is headed. While Apple itself operates as a walled garden (including a set of NFC patents), the application provision market for open Google Android, Blackberry and other handset operating systems ensures that complete payment choice—and self-sufficiency—is a safe bet among smart phone users (28% of the marketplace at year-end 2010).<sup>35</sup>

For some of these companies (e.g., PayPal, BlingNation, Obopay, and Western Union), capturing incremental payments *is* the business model, and gaming payment fees drives the business case. For the most part, these companies gain merchant and bank acceptance at slightly lower fee levels than standard signature-based cards. In a post-Durbin world, however, there is no certainty that these base-level rates will prove sustainable. So even they will need to find other sources of revenue in the value they add.

For online marketers morphing to the mobile environment, such as Google, marketing sources of revenue—i.e., paid searches, lead generation fees, linked advertising, etc.—promise to be as rich as on the internet. In fact, in their previous payments foray for the online market (Google Checkout), the search goliath attempted to make payments transparent to the advertising and marketing propositions—a useful analogy for mobile, perhaps.

---

<sup>35</sup> Composite estimates of CTIA, ABI Research and other industry research firms.

Moreover, the ability to add real-time, location-aware, one-to-one granularity to essentially 'blind' online interactions offers the potential for much higher fees and profits from results superior to those online. Such optimism is borne out by the surging number of mobile coupon tests being conducted in the marketplace. Initial results of user take-up appear very encouraging for all participants—including merchants which appear willing to pay high rates for consummated purchases than can be demonstrated as incremental and/or taken from competitors.

#### *Technology Providers*

Most of the other components of the mobile payments ecosystem sell infrastructure and/or related services to the others. Such technology includes handsets, security components, communications and systems integration, and even shared-services configurations such as Trusted Services Managers (TSMs). Most of these participants are dependent upon a fully secure, two-way NFC paradigm becoming commonplace in the next 2-3 years. Accommodating secure payments is viewed as an essential baseline service that will attract the consumer to other high-value activities, and that, in turn, will further increase demand for their products and services.

To some degree, these participants can 'prime-the-pump' for new infrastructure. For example, Nokia's announcement in late 2010 that all of its smart phones from 2011 forward would be full NFC-enabled help dilute skepticism that an NFC critical mass would ever appear. Google's recent announcement that Android 2.3 would support NFC payments, coupled with reports that millions of NFC-enabled phones were already in the Android pipeline, further buoyed confidence and expectations in this ultimate baseline configuration for mobile payments.

To-date, mobile technology providers tend to embed their products and services in packages crafted by the carriers, and more recently by Apple, Google, and Microsoft—as these computing companies expand their presence into the mobile marketplace. The real costs of this technology (e.g., full NFC components for GSM handsets is believed to cost an incremental \$5-\$10) is often not visible to the public, but must be accounted for in a business case for *some* member of the mobile payments ecosystem. But that business case does *not* have to be based on payments functionality alone.

#### *Regulatory Road Map/Shared Infrastructure Decisions*

All of these uncertainties make business planning precarious, and companies hesitant to invest. So representative constituencies of *all* of these participant groups have asked the Fed to coordinate with other regulatory agencies (such as the FCC and FTC) and provide a 'regulatory road-map' of what functions, activities, and implementations would be viewed as permissible over the next three to five years. These mobile payments ecosystem players are also asking for clarity on what infrastructure can/should be shared on a non-competitive basis.

For example, security is certainly a foundation for market cooperation, as evidenced in TSMs for smart cards worldwide. But other business services that might be critical to market adoption in the U.S., such as standardized contracting among 16,550 banks and credit unions, 5,000 wireless carriers, and millions of merchants, notification services for lost handsets and even (perhaps especially) coordinated risk management are all under consideration.

So the foundational notion that has emerged is to compete on the marketing and personal service value propositions—but not on generalized transaction capabilities. In this sense, payments become a *qualifying* factor for standardized applications and components of shared infrastructure that protect everyone, but the mobile marketing, advertising and promotional components become the bases for *differentiation* (and therefore competition). As such, mobile marketing services become the heart of the business case for NFC payments. (Note: This is really a good point. Let's see if we can incorporate it in the new vision part of the document also.)

Thus, the mobile marketing business case drivers—mostly still to be determined in an empirical way—should be viewed, and researched, as part of a brand new theoretical construct. Under this construct, payment choice, with open and/or interoperable mobile wallets, will enable the market to set its own prices—in all likelihood as a function of actual costs. And superior customer value in facilitating efficient and effective transacting should engender contributions (financial or otherwise) from both buyers and sellers for the new value they receive. Whether that value materializes as purchase commitments from consumers, or incremental purchase bounties from merchants, the specific mechanism is less important than the concept that real value provided will find a path to fair compensation.

**APPENDIX IV – Mobile Payments Standards in the U.S.<sup>36</sup>**

Mobile payments require multiple industry participants to work together. If collaboration is difficult, adoption will be delayed. Difficulty may arise because the industry is made up of many small participants who are heterogeneous and have very different preferences, because there is a culture of distrust, or because of legal restrictions. All of these issues play a role in the evolution of mobile payments.

Because there are over 16,000 banks and credit unions but just four major mobile carriers (who account for nearly 90% of the handsets used) in the U.S., industry-wide agreements on technology standards and business policies are very difficult to coordinate and negotiate to reach consensus. Bilateral negotiations between a single bank and a single carrier are much easier, but the market share of customers having accounts with both the bank and the carrier for any given pair of institutions is likely to be small, lowering the value of any resulting agreement. The number of parties involved in each transaction: a mobile carrier, a handset manufacturer, a payment network, a mobile software vendor, a bank, a merchant, and a consumer also make it more difficult. The parties must agree on who is responsible for verifying the consumer's identity, resolving disputes, handling customer service, etc.

Coordination problems may be exacerbated by the possibility that the significant players (banks and mobile carriers) both consider the users to be their customers and therefore may want to "own" the relationship with the customer and the rich set of information that mobile payment services yield.<sup>37</sup> And even though four mobile carriers dominate the wireless market, there are 5,000 wireless carriers in the U.S. in total. Nearly all are small, localized carriers that serve customers in rural areas of the country. The FCC does not want those rural carriers to disappear as the industry evolves, so it will be important to integrate them into the mobile ecosystem.

Open industry-wide standards, involving all stakeholders, are necessary to achieve mass adoption of mobile payments. The alternatives are not simple. For instance, mobile carriers could offer payment services without the involvement of banks, perhaps by limiting consumers to pre-pay accounts or by offering consumer credit themselves. Alternatively, a single carrier could contract with a single bank to offer payments services. These types of approaches are feasible, but they face serious hurdles. Limiting consumers to pre-pay accounts reduces the attractiveness of the product, and offering credit services brings carriers into an unfamiliar industry at a large scale, with important regulatory obligations. To succeed on a large scale by contracting with a single bank, consumers must agree to transfer their financial relationship across institutions, something they are often hesitant to do.

---

<sup>36</sup> Excerpts from Crowe, M., M. Rysman and J. Stavins. 2010. "Mobile Payments in the U.S. at Retail Point of Sale: Current Market and Future Prospects." Federal Reserve Bank of Boston Public Policy Discussion Paper, No. 10-2.

<sup>37</sup> McCarthy, B. 2008. "Mobile Payments: The Linchpin of the Mobile Commerce Economy," White Paper, First Data.

The U.S. is making important progress in developing an industry standard for the technical details for how mobile payments might work, thus overcoming substantial negotiation costs in this regard.

#### *Current Mobile Standards Efforts*

The development of open industry-wide standards through collaboration of industry stakeholders may be the best path towards successful adoption of mobile payments. Importantly, an open standard for mobile payments is under development currently. The financial industry standard-setting group ASC X9 is developing U.S. standards, and ISO is developing an international version of the standards.<sup>38</sup> The X9 and ISO standards will specify how a mobile phone securely formats messaging and data elements and delivers that information over payment rails. Any bank, mobile carrier, or other vendor that develops its service in compliance with the standards would be able to participate in the mobile payments market. At this stage, prospects for the ultimate development of mobile payment standards appear to be strong, although their readiness is at least 18 months away. However, developing a standard does not ensure that it will be adopted.

Although standards are currently in place for the transmission of data either remotely or by proximity from a mobile device to allow for mobile commerce, gaps exist and need to be addressed in order to provide an efficient and secure mobile commerce environment. While ISO 14443 describes the physical characteristics of proximity hardware and NFC standards enable the exchange of data wirelessly, the following work efforts are underway to address the gaps.

#### *ISO TC68/SC7/WG10 Mobile Banking / Payments (International)*

The ISO study group, convened by the U.S., has identified areas for development of an international standard and will be formally developing standards for the following areas:

- Mobile person-to-person payments, involving a financial institution intermediary
- Life cycle management of banking/payment applications
- Banking alerts
- Banking account Inquiries
- Banking solicitations and offers
- Payer to the secure element authentication
- Discovery of device capabilities
- Technical report on business oriented security requirements

---

<sup>38</sup> ASC X9 (Accredited Standards Committee X9) is an industry nonprofit association composed of members of the financial services industry. ISO (International Organization for Standardization) is a network of national standards institutes of 162 countries, one member per country. It is the world's largest developer and publisher of international standards.

For the new work item, the group recognized that Payments break down into two broad areas, proximity and remote. There is a consensus that models for point-of-sale payments will heavily leverage the standards in place for NFC contactless payments. The workgroup will set new standards for “Life Cycle Management of Banking/Payment Applications” as well as “Person to Person” payments, including remittances, focusing on mechanisms that leverage clearing and settlement through established banking channels. These standards will include messaging between parties as well as bill and invoice payments.

For banking the workgroup will focus on three areas: “Alerts,” “Inquiries” and “Solicitations/Bank Offers.” Each will leverage existing standardized technologies, e.g. Short Message Services (SMS), Instant Messaging (IM) and Really Simple Syndication (RSS). For authentication, the workgroup will develop standard interaction models for “Payer to the Secure Element,” standard means for the identification of “device capabilities”, and document “business oriented security requirements” for sound banking practices.

#### *X9.112-3 - Mobile Commerce (Domestic)*

The mobile environment accumulates numerous risk factors, such as: unattended terminals, card-not-present transactions, untrustworthy platforms, and persistent wireless connections. Further, the mobile network operator (MNO) infrastructure may not provide sufficient security that can be relied upon by the financial services industry. From a security perspective mobile commerce suffers all of the same vulnerabilities as the internet and wireless environments combined; and from a business perspective it encompasses three disparate industries: financial services, mobile telecommunications, and manufacturing mobile platforms.

Areas within scope of this standard include but are not limited to the following:

- Mobile transactions, including sending and receiving messages for payments, banking, and commerce
- Mobile payments for person to person (P2P), person to business (P2B), and small business to business (SB2B), including credit card, debit card, and electronic funds transfer (EFT) transactions

Areas not in scope because they are addressed by other ANSI or ISO standards include: PIN Management and Security; Biometric Information Management and Security; Key Management and Security; and mobile marketing (e.g. advertisements, coupons, loyalty programs, catalogs).

## **DEVELOPING THE FRAMEWORK FOR SAFE AND EFFICIENT MOBILE PAYMENTS—PART II**

**TUESDAY, JULY 10, 2012**

U.S. SENATE,  
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS,  
*Washington, DC.*

The Committee met at 10:02 a.m., in room SD-538, Dirksen Senate Office Building, Hon. Tim Johnson, Chairman of the Committee, presiding.

### **OPENING STATEMENT OF CHAIRMAN TIM JOHNSON**

Chairman JOHNSON. Good morning. I call this hearing to order. Today's hearing is the second in a series of hearings that will examine the mobile payments marketplace. Building on the information collected at the first hearing, this hearing will focus on the benefits of mobile payments to consumers and businesses as well as the obstacles to adopting this new form of payment. As discussed at our first hearing, this Committee's jurisdiction extends over all financial services and payment systems regardless of the company that delivers the service.

Today's panel of academics is at the forefront of mobile payments research. Each has spent much time studying this topic either through an economic or legal lens. They will discuss the benefits of mobile payments including, among other things, enhanced data privacy and fraud protection, consumer convenience, expanded access to mainstream financial services for the underbanked, merchant cost savings, and streamlined marketing and promotion opportunities.

Additionally, we have asked them to discuss obstacles to adopting mobile payments. Some potential barriers to adoption are levels of consumer awareness, information security, fraud and privacy concerns, compatibility of business models, development of industry standards, deployment costs for merchants, and regulatory uncertainty.

The bottom line is that as the mobile payments system evolves, it is important for this Committee to understand how they work in order to provide proper oversight so that these payments can be secure and convenient. I look forward to today's testimony.

I want to remind my colleagues that the record will be open for the next 7 days for opening statements and any other materials you would like to submit.

Now I will briefly introduce the witnesses.

Michael Katz is a professor of economics at the University of California, Berkeley, and the Sarin Chair in Strategy and Leadership.

Sarah Jane Hughes is a university scholar and fellow in commercial law at the Maurer School of Law at Indiana University.

And Thomas Brown is an adjunct professor at the University of California, Berkeley School of Law.

I thank you all again for being here today. I would like to ask the witnesses to please keep your remarks to 5 minutes. Your full written statements will be included in the hearing record.

Mr. Katz, please proceed.

**STATEMENT OF MICHAEL L. KATZ, SARIN CHAIR IN STRATEGY AND LEADERSHIP, PROFESSOR OF ECONOMICS, UNIVERSITY OF CALIFORNIA, BERKELEY**

Mr. KATZ. Chairman Johnson, thank you for inviting me to appear before you today to talk about mobile payments.

As everybody knows, America's consumers are increasingly connected via smartphones, tablet computers, and other mobile devices. A lot of people have predicted that this is going to lead to a revolution in how people pay when they go into a bricks-and-mortar merchant. And, in particular, what people are focusing on is near-field communication, which is a technology that allows your phone to communicate with the merchant's point-of-sale device so that you can swipe your phone the way people today swipe credit and debit cards.

I disagree with those who think it is going to revolutionize payments. Just to put it in short, near-field communications is about communications that happens at the 1- or 2-foot level when you are actually at the checkout. But I think the really interesting and exciting developments here are really about what happens when the consumer is in the neighborhood of the merchant, because your mobile phone gives the merchant a way to know that you are there because of location-aware services and then to reach out to you and encourage you to come into the merchant.

So I think there is going to be a revolution in mobile payments that is going to spring from smartphones and tablets, but that revolution is not going to be in the way we pay, but it is going to be in the way that merchants interact with their customers.

Let me step back for a moment and ask how we are going to get from where we are today to where I think we are going.

Today, merchants and consumers already have access to a wide range of options. They have got cash and checks, credit and debit cards. These options are easy to use, they are widely accepted, and, importantly, they are trusted. Moreover, most consumers already have established relationships with payment service providers, and merchants have made substantial investments in equipment, systems, and training to support existing payment services. So if new payment services based on smartphones and tablets are going to compete successfully, they are going to have to offer merchants and consumers additional value when compared with current options. Cool technology alone is not going to be enough.

Now, from the merchant perspective, mobile payments will be attractive if they do one of two things, and ideally both: one would

be to lower the merchants' costs of completing transactions, say by charging lower fees to the merchants or somehow speeding up the checkout process; the other benefit, and the one I want to focus on because I think it is potentially much larger, is attracting additional consumer patronage.

So how will mobile payment services attract customers to bricks-and-mortar merchants? Survey research shows that what consumers want are payments that are widely accepted, are easy to use, and are trustworthy. So how do mobile payments stack up against the competition?

When it comes to paying at bricks-and-mortar merchants, the extent of acceptance is a weakness rather than a strength. Indeed, mobile payment services face a chicken-and-egg problem. Specifically, a merchant does not want to bear the expense of changing its checkout process to accommodate a new payment service if there are few consumers who use that service. Similarly, a consumer does not want to sign up for the payment service if very few merchants accept it. But, of course, if everybody waits for everybody else to join the new payment service first, it is never going to get off the ground.

Now, there are several potential solutions to the chicken-and-egg problem, but all of them rely on one common underlying factor: There has to be some source of benefit that makes it worthwhile to invest in overcoming the chicken-and-egg problem. So we are back to looking for a source of consumer value.

Now, an NFC-enabled digital wallet can be more convenient and possibly easier to use than a conventional wallet filled with multiple payment cards. But it should be noted that we are not going to be able to give up our conventional wallets anytime soon because we still need our wallets to carry our driver's license, insurance cards, and things like that. Once those go digital, we may have a different situation, but right now we do not.

Moreover, we have to ask ourselves: Is it really that much easier to swipe your phone than to swipe a smart card? So I believe in the short run that ease-of-use benefits are going to be too limited to be a significant driver of adoption.

So that leaves trust as a source of value. Security and privacy are two elements of trust. Consumer surveys show, unfortunately, that people question the security of mobile payments, and indeed mobile payment systems do have points of vulnerability, such as the radio interface, that card-based systems do not. Moreover, through the use of malicious code downloaded through apps or Web browsing, a smartphone can be compromised without the attacker's having to attain physical proximity. Consequently, security is not going to be a positive driver of mobile payment adoption anytime soon. And, unfortunately, things do not look a lot more promising for privacy. Consumer surveys show that many consumers are worried that mobile payment companies will collect too much information and that they are going to misuse that information.

So if we come up short on ubiquity, ease of use, and trust, where is the value that is going to drive these things? I think the answer is, as I said at the beginning that the way merchants are going to use the capabilities that mobile phones bring and mobile payments do, is to collect vast amounts of information about consumers, ana-

lyze that information to develop predictions of consumer behavior, and then use that information and the ability to communicate with their customers to deliver personalized, real-time, context-specific messages to encourage consumers to come into the store.

Let me close by just giving an example of the possibilities you could have with this. You could have a coffee retailer get an alert from a service provider saying, you know, here is one of your regular customers. Normally by 10:30 she buys a cup of coffee. However, today it is 10:45, she still has not bought a cup of coffee, but we notice she has just left her office. Do you want to send her a message encouraging her to come into your retailer that is three blocks away? The retailer could check its store, find out that it is not very crowded, check the fact it is a hot day, and send a message to the consumer saying if you come into our store in the next 30 minutes, we will give you 20 percent off on an iced coffee. That is an incredibly powerful potential marketing tool, and that is where I think the real benefits and the real power of mobile payments are going to lie. I think we will see NFC in the future, but it is really going to be something that is an extension of existing payments. It is not the revolution.

Thank you.

Chairman JOHNSON. Thank you, Mr. Katz.

Ms. Hughes, please proceed.

**STATEMENT OF SARAH JANE HUGHES, UNIVERSITY SCHOLAR  
AND FELLOW IN COMMERCIAL LAW, MAURER SCHOOL OF  
LAW, UNIVERSITY OF INDIANA**

Ms. HUGHES. Senator Johnson, thank you so much for the invitation to be here. Other Members of the Committee, I appreciate this opportunity.

Dr. Katz has already raised a few of the issues that I would have covered, and I had broken my prepared remarks down into five points that I thought offered benefits and five points that I thought changed compliance costs or otherwise imposed some obstacles to the adoption of mobile payments by merchants. So I may edit my remarks in order to take advantage of what Dr. Katz has already given to the Committee, but the Committee has my full statement.

I would also like to flip from the end of my remarks a point that I want to be certain to make, and that is that, in thinking about regulating mobile payments, I think it is important to recognize that this is probably not a one-solution-fits-all-possible-providers situation. So that the banks, the telecom providers, the app providers, intermediary payments processors, and merchants all may have the need for certain protections and rights, and the customers in dealing with them along this pathway of multiple players in a single-payment transaction. The disparities in the roles that they play in mobile payments could be recognized in suitable forms of regulation, but it is vital that we not create a situation—and we may have it now—where one form of regulation drives people into unregulated silos or channels of opportunity or where they can go to silos that are less regulated and save a lot of compliance costs. So that if you are going to regulate, you need to think about how to do it in a way that does not reward a certain group of players

at the expense of merchants and consumers and competition in general.

Now, returning to the five or at least an edited version of the five pros and the five expenses. Dr. Katz has already made the case for mobile payments possibly being quick and having certain functionality, and I agree with him. I think that there is a second-level point, and that is, taking mobile payments has a particular potential benefit to small business owners because it allows them to collect sums from consumers, and this may help them expand their roles in the economies. This may be particularly true for small-dollar payments as opposed to large-dollar payments, and I think that it is also true that trust plays a factor.

In the cab coming here today, I noticed the cab driver's willingness to talk about paying for a \$2 cup of coffee but his reluctance to think about making a \$200 car note payment with a mobile device at this point. So we will see how this expands.

The third is that there is a lot of talk about mobile payments helping merchants deter fraudulent charges—and the customer as well—because each of them gets a real-time signal. That may or may not be the case, but it is something for us to think of as a potential benefit.

I agree with Dr. Katz that there are huge opportunities, indeed perhaps the most important opportunities, to build customer loyalty, to do geolocation in individually directed marketing to customers, that those are far ahead of anything that traditional payments have had to offer.

We also have something Dr. Katz did not talk about: merchants' abilities to reach consumers who do not have checking accounts—they are unbanked—or those who are in areas where there are relatively few banks and where access to an ATM machine may be more scarce than it is in major metropolitan areas. I spent some of my childhood in Missoula, Montana. I spent some of my childhood in Butte, Montana. My mother was born in North Dakota and spent some of her childhood. It is a long way to an ATM in some parts of this country. In Bloomington, Indiana, it is not, but in other places it is a really long way, especially to a branch of a financial institution these days.

The unbanked and underbanked use smartphones right now to make certain kinds of payments because it helps them have access to the marketplace that people who live in metropolitan areas already enjoy.

So Dr. Katz has talked about the fact that mobile payments have interception risks and malware problems and all of those things, that they allow harvesting of information, but they do not relieve merchants of the costs of compliance with chargebacks, with other security costs, of payment data, integrity concerns, and by that I mean protection against alteration, replication, or misdirection of payments, of the time to explain to consumers the kinds of issues involved in making mobile payments if the consumer is not familiar, and they do not talk about the added risks that the banking industry is concerned about of many more people being able to access and maintain consumer deposit or checking account information.

My last point is one that your invitation specifically asked to have addressed, which is that taking mobile payments will require merchants, and others in the process, to have to think about whether they are supposed to comply with privacy laws, with record retention laws, and with laws that are designed and regulations that are designed to deter and detect money laundering and terrorist finance, including dealing with countries we are not supposed to deal with, and specially designated nationals who are kingpins in the drug industries or gun running and the like.

With that, Mr. Chairman, thank you.

Chairman JOHNSON. Thank you, Ms. Hughes.

Mr. Brown, you may proceed.

**STATEMENT OF THOMAS P. BROWN, ADJUNCT PROFESSOR,  
UNIVERSITY OF CALIFORNIA, BERKELEY SCHOOL OF LAW**

Mr. BROWN. Thank you, Chairman Johnson, Ranking Member Shelby, and Members of the Committee. I very much appreciate the opportunity to come and address the subject of mobile payments with two distinguished colleagues in academia, Professor Katz and Professor Hughes.

Like Professor Katz, I believe that mobile payments are going to revolutionize the way commerce takes place, and like Professor Katz, I do not believe that that is a revolution that will begin at the point of sale in brick-and-mortar stores. Rather, I believe that mobile technologies are changing the way people accept payments fundamentally.

It used to be a really complicated thing to have the opportunity to accept payments. Today, anybody pretty much anywhere can get a mobile reader in a little packet like this, download an app, plug the device into their phone, and accept payment cards on a mobile device. All of the misery associated with complying with the contractual process imposed by the card networks and the banks has been largely eliminated. This is a fundamental change in how consumers and merchants have the ability to interact.

Most payment applications from a consumer perspective—and I have two that have been around for a while: cash, which I am sure most people here are familiar with; and payment cards, which I suspect most people are also familiar with—are, from the standpoint of a consumer, mobile. Most of us carry our wallets wherever we happen to be, and in those rare instances where we do not have our wallet, we tend to notice it and try to find it.

The really profound change associated with mobile payments is that we now carry point of sale devices with us at all times. This is bringing lots and lots of merchants into the electronic payment infrastructure square into it, and others have signed up—literally millions of informal merchants—to accept electronic payments. That is one important change.

The other change is how it is affecting how established merchants interact with their customers. Professor Katz talked about the interaction with customers in the store or near the store. Now, instead of having to check out at the point of sale, we can make our purchases in the aisle. We can also make purchases outside of the store. One of my favorite mobile payment applications is the Apple Store app, not to be confused with the App Store, which you

can also download and access through the Apple Store app. It turns your mobile device into a mobile checkout. So I can be outside of the Apple Store, identify purchases that I want to make, make the purchase through my mobile device, take the item off the shelf when I show up at the store, and walk out without ever having to present a payment credential at the point of sale.

These changes are what is truly revolutionizing commerce, bringing together industries that we used to think of as entirely separate—telecommunications, financial services, and retailing.

What are the implications? Well, this revolution raises a number of different questions. The first—and it is a natural one—is: this is new, so we must have to regulate it. The second is concerns about privacy because, obviously, all of these transactions involve the flow of information, and we know or we have a sense that these mobile devices gather a lot more information about us than other ways that we are used to engaging in commerce. And then, finally, there are questions of compatibility, and let me try to briefly address all three of these.

With respect to existing regulation, let me assure the Committee: the payment industry, and the mobile payment piece of it, is heavily regulated. It is heavily regulated both at the Federal level and the State level. A mobile payment provider confronts some very important choices about how they offer their products. They can obtain licenses at the State level, or they can contract with an existing chartered institution who will sponsor their payment application.

But those are just table stakes. If you then want to offer that product to consumers, you confront a long list of Federal and State requirements. I am not going to go through all of them, but we are all familiar with them, hopefully: TILA, the EFTA, the Bank Secrecy Act, OFAC. Offering a consumer financial services product in this country is a very complicated proposition. We do not need new rules.

To the extent that we want to decrease barriers to entry and increase innovation, I would suggest that Congress attend to the complicated regulatory and licensing issues that exist at the State level. Whatever benefit might exist from State licensing is completely eliminated by having each State license every payment provider in the United States.

Second, privacy. Professor Katz uses a wonderful example of somebody who goes to a coffee store and then misses their daily appointment and receives an offer. Well, it does not take a huge leap of imagination to think through an example that might make us a little uncomfortable, which is, instead of receiving an offer from the cafe that you generally visit, you receive an offer from the doughnut shop across the street that you have never visited. Although we might like the first kind of offer, I think the second offer seems a little creepy. That creepiness instinct tends to vent itself in wanting to prevent people from sharing information. I want to suggest that that is not the answer, and the reason can, I think, be found in a couple more hypotheticals. Instead of imagining somebody missing their appointment in the city and receiving an offer from someplace across the street, let us suppose that the person is in a new city, and they receive an offer from a merchant who

says, "We know that you like Blue Bottle Coffee back home in San Francisco. Why don't you try Elixir in Philadelphia? We think you will be happy."

The first offer might make us feel a little uncomfortable; the second offer, maybe not so much. And regardless of how concerned we are about the extent to which one offer seems creepy and the other does not, restricting the sharing of information, which tends to be the framework that we use for most privacy legislation in the United States, does not prevent the offer from being made. It simply encourages the firms to merge or to integrate.

If people cannot share information that is then used to support mobile payment applications, what that leads to is firms combining under a single roof. So, if the doughnut store owner and the coffee store owner are owned by the same person, then you can receive the offer, but not if they are separate. I think instead of focusing on sharing, we should focus on consequences.

And that leaves me just a little bit of time to discuss compatibility. This is a very complicated subject. I will not go into it in detail. I will say compatibility problems can be a concern. They might not be a concern. There is no one-size-fits-all solution to them. Fortunately, we have a legal framework in the United States that addresses these issues quite well in the antitrust laws.

Thank you. I am more than happy to answer any questions that you might have.

Chairman JOHNSON. Thank you for your testimony.

As we begin, I will ask the clerk to put 5 minutes on the clock for each Member.

Mr. Katz, what is the biggest obstacle to widespread adoption of mobile payments by consumers and merchants? And how can it be overcome?

Mr. KATZ. I think there are two levels at which to answer that. I think at one level the biggest obstacle is the lack of real value right now given that we in the United States have so many payment instruments that work extremely well. We have very well developed credit and debit markets, so we have tough competition. And so where that shows up, I think, is really this chicken-and-egg problem, that everyone wants to wait to see everybody else get onboard with the system. And there are solutions to that, as I mentioned, so let me just say a couple words about it.

One of the things that will help, as Mr. Brown was saying or touched on, is compatibility, and I think we will see compatibility in point-of-sales devices. I think once we get onboard with that and see point-of-sales devices that work both with mobile phones but also with existing smart cards and work with the Visa and MasterCard systems in particular, I think then we will see merchants start adopting these things, and that will give us a path going forward.

Chairman JOHNSON. Ms. Hughes, how would you expect small merchants to be affected by widespread adoption of mobile payments? Are mobile payments providers likely to compete in cost with existing payment providers to the benefit of small businesses?

Ms. HUGHES. Mr. Chairman, I think the small business providers are already beginning to realize some of the benefits of mobile payments. Ice cream shops, people who have transactions, many trans-

actions—coffee shops, doughnut shops—of \$10 or less are seeing the application such as the one Mr. Brown suggested—I am borrowing your prop—where the reader is on the phone or where it is possible to tap the phone in close proximity to another reader and have the information be shared.

The costs of using a system such as the one Mr. Brown mentioned, Square, is considerably lower than what is happening in a comparable transaction using a credit card or debit card rail right now. I am on the board of a tiny nonprofit, and last year, because of our interest in trying to save costs, we switched to Square, and we reduced our average transaction charge by about 1.05 percent per transaction. So, in other words, instead of paying about 3.75 percent in interchange fee, our end, for the transaction, we paid about 2.7 percent for the transaction.

The other way in which this helps small businesses, it helps artisans and craftsmen, it helps farmers at farmers' markets, places where they do not often have electrical support for their credit card processing machine, but they do not want to just use plain old paper credit card slips because they cost more to process, and the amounts of the sales are often not enough to support the fee that will be charged in the traditional debit and credit modes.

So there are cost savings, to which Mr. Brown alluded in his remarks, and I thought quite well, but without the specificity of the example that I have just offered for this purpose.

Chairman JOHNSON. Mr. Brown, when a consumer makes a mobile payment, what information is collected and what is the information used for? With whom is the information shared, and do consumers have a say? Should there be limits on the information that is collected and how the information is used? That is a mouthful.

Mr. BROWN. It is, and I notice we only have 2 hours for the hearing.

[Laughter.]

Mr. BROWN. I am not going to try to answer it in all of the detail. It is a question that goes to the heart of what is happening with mobile payments, and let me try to answer it by identifying a couple of different ways in which mobile payments happen.

Professor Katz has talked a little bit about NFC applications. The most familiar is the Google Wallet that you can sort of wave at and tap on a phone to execute a payment in a brick-and-mortar environment. I have talked a little bit about the mobile devices and mobile shopping cart. So these are two sort of archetypes for these kinds of transactions, and the information that is collected and processed in connection with these transactions is different.

When the mobile phone is being used simply to replace the swipe from a payment card, for all intents and purposes, the only information that is being passed among the parties to the payment itself—so merchant, processor, network, issuing bank—is the information associated with authorizing and settling that payment.

When the mobile device is being used as a shopping cart, so we're essentially taking a payment application and combining it with the ability to fulfill purchases, there is a lot more information that may be hosted or held by various participants in the chain associated with the delivery of that experience to the customer.

So what does that mean? We can take Amazon as an example. Amazon has a mobile Web site that you can visit on your mobile device and through which you can make a purchase. We often think of Amazon as the merchant associated with those transactions, that is, that Amazon actually owns the good that it is providing to the consumer. In fact, Amazon acts as a platform for a number of small merchants who are selling through the Amazon mobile Web site. And when you make a payment to Amazon, Amazon processes that payment and then delivers it to the merchant.

Amazon as the processor and platform in that example often hosts the shopping cart information and then uses that to, among other things, make recommendations when you visit the Amazon platform.

So the short answer to the question about what information is taken and how it is used is there is no single answer, but hopefully those two examples give some sense of the differences.

Do consumers have a say? This is a very interesting question. And the answer is, for the most part, when you are using the mobile device as a shopping cart, with Amazon, with Apple, with most of the other mobile shopping cart examples that I can think of, the terms of service from a consumer perspective with respect to the use to the consumer do have a provision that explained to the consumer, at least in some sense, how the host or provider of that service can use the consumer's information.

I think that then leads to the next question. What rules exist with respect to the enforcement of the promises that are made? And should there be regulation with respect to the collection of the information? So let me talk about enforcement first. And the answer is yes, we actually have an enforcement mechanism for that. That is largely what the FTC has done in its privacy enforcement efforts. There was an article in today's *Wall Street Journal* about an enforcement action currently pending before the Commission related to Google and Google applications that subvert or go around the privacy provisions that are built into the Apple app store. So this provides an example of how existing law is being used to police consumer expectations with respect to how the information is being used. But this is a very complicated set of issues.

Chairman JOHNSON. Senator Merkley.

Senator MERKLEY. Thank you, Mr. Chairman, and thank you to all of you for your testimony.

I wanted to start, Professor Hughes, with your point about how mobile payments can help the unbanked and the underbanked, and specifically if you could share any more thoughts about how we make sure that mobile payments become a pathway to financial services that are healthy, if you will, and supportive to this underbanked or unbanked community versus being a pathway to predatory practices that we have seen plenty of times in other venues.

Ms. HUGHES. That is a very interesting question. Thank you. The adoption of smartphones by underbanked persons is one of the most interesting phenomenon in this whole space because many people who are underbanked do not—they are either underbanked because they live in locations where there are not very many depository institutions from which to choose or they do not really

have enough money to sustain an account or they have lost the privilege of having one.

The unbanked are in a similar situation, but they may never have had a checking account because they could never afford it or because they have come to the United States from places where the banking system was not well trusted.

As a result, smartphone technologies replace two very important functions in a contemporary American resident's life: access to the Internet and access to financial services. Those are so powerful forces in our economy at this point that it is very important to protect, as you have suggested, access and to hope that access will be on terms and conditions that respond to needs and are not unfair or deceptive in the way in which they are applied.

The cost issues for the consumer after you acquire the device that you are going to use—the tablet, the smartphone, or whatever—may be very similar from the consumer's perspective to the cost that the consumer would have if the consumer had to go and get dollars, had a credit card, which they may not have because sometimes those take large up-front fees or deposits or things that these consumers may not have.

So just as it looks to us like we process checks at par but the costs are really embedded in the system, the costs here are embedded in the system. And with credit and debit transactions, they may, in fact, be buried.

So the consumer may or may not incur more costs, but if you think of the time savings of not having to go to the ATM, not having to carry cash, assuming that you have an ATM to go to, not paying a fee to cash a check if you were paid by check or a fee to get your money out of your payroll card account if you have been given a payroll card account, the opportunity to load your payroll into your mobile device and use it as a replacement access mode like a check or a credit or a debit card for monies that you may have on deposit other places are all enormous.

It is a huge marketplace. There are at least 30 million adults in this country who do not have adequate bank access. I think the number is considerably larger than that, but the figures I see talk about at least 30 million. Some have projected as many as 50 million people in the country who do not have access to banking accounts.

Senator MERKLEY. Thank you, Professor, and I will not ask you more on this. I will just note that we have plenty of challenges with, for example, prepaid debit cards that then have all sorts of hidden fees. You acquire a balance, and you pay \$20 if you use the card for the first time. You pay \$20 if you use it. Every month you pay \$20, or whatever. It is continuous fees. And I can see those being very hidden, even more hidden, if you will, in the context of an electronic platform, and we could end up with a world that expands with very expensive costs to working people. And we also have the potential for solicitations for payday loans that are 300 percent interest, 500 percent interest, where it is, you know, click here and the first thing you know you have got a very expensive loan that you did not have a full sense of that you might have if you had to go to a brick-and-mortar location and discuss it.

So it is just kind of a thought that we should have that in the back of our mind as this powerful new frontier—as we enter it.

I want to switch gears a little bit to Professor Brown, and if I understood your comment correctly, you were arguing against any restriction on the sharing of information between groups that collect that information on consumers, arguing that it simply encourages, if you will, a horizontal ownership structure. My first kind of reaction to that was a little bit of doubt about the argument you were making in that if I have a company that I am dealing with that I can check out their privacy policy, I have at least some instrument as a consumer to pick and choose ones that have a privacy policy. But if there are simply no restrictions on their sale of my information, I have lost any ability to control that or to respond as a consumer to the different offerings from different folks. If I could just get a little more sense from you on this.

Mr. BROWN. Sure. What I want to emphasize is that I think with respect to privacy and information security, we should focus on bad consequences, identify those, and think of ways that we can minimize their potential for arising and minimize the potential that the party that is in the least position to avoid them ends up bearing the consequence.

So let me give you some examples of this. The Do Not Call list is an example. The caps on liability to consumers for unauthorized transactions under Reg E and Reg Z are other examples of this.

With the Do Not Call list, many of us do not want to receive calls that interrupt our dinner, and this is a totally natural thing. We do not like to get them in the Brown household either. Those calls originate not because my telephone information is collected and shared by merchants, but because my telephone number can be auto-dialed by somebody. I am allowed then to identify my number as a number that should not be auto-dialed. That is a focus-on-consequence approach. Reg Z and Reg E do much the same. With Reg Z, if there is an unauthorized transaction on my credit card, my liability is capped at \$50 when I provide notice to the credit card company. As a consumer, once my information is out there, there is not much that I can do to prevent somebody else from obtaining it and then using it in a fraudulent manner. So I am not what we would call in the common law, the least cost avoider. There are other people in that payment stream—the merchant, the network, the bank that issued the card, the merchant that subsequently accepts my information—who are all in a better position to avoid that transaction than me.

Senator MERKLEY. I see your point, and you are arguing in favor of the equivalent of do-not-call-type strategies that, regardless of who has the information, which is a powerful tool for consumers.

Mr. BROWN. Right, because I think focusing on sharing just leads us into things that end up not helping people. Gramm-Leach-Bliley is the best example. We get these long notices every year that no one reads, and we think that we are protecting people's privacy interest, but, all we are really doing is giving a subsidy to the post office—which may itself be useful but is not necessarily advancing the privacy interests or this creepiness concern.

Senator MERKLEY. I do think the post office is happy about that. [Laughter.]

Mr. BROWN. Yes.

Senator MERKLEY. Thank you.

Chairman JOHNSON. We will proceed to a second round.

Mr. Katz, I will ask you the same question as I asked Mr. Brown. When a consumer makes a mobile payment, what information is collected and what is the information used for? With whom is the information shared? And do consumers have a say in it?

Mr. KATZ. So as Mr. Brown was saying, that is indeed a complicated question and a more complicated answer. Let me amplify a few of the things he said.

The actual payment transaction does not necessarily provide any additional information at all compared to a traditional credit card transaction. But one of the things that could really change things when we are talking about mobile is that there is a lot of other information that goes along at the same time that you typically do not have with a credit card.

So, for example, although you can infer the customer's location from where he or she used a traditional card—and, in fact, Visa has a system now that does that and sends you a message because Visa knows where you are using your creditor. With mobile payments and GPS-enabled phones, there is way more ability to track people.

But I think in all of this, it is not so much the change that there is going to be more information collected. Credit card companies have unbelievable amounts of information about us today. In fact, unfortunately, I went through something where someone in my family had stolen something from us and run off to another State, somebody we had been taking care of. We ended up determining who our friends were that we did not know existed before, what State she had run off to, where she was living, how she had gotten there because we had a trail of gas station receipts. We were able to build a really detailed picture of this person's life, and this was something that happened 15 years ago using credit card information.

So the information is already out there. I think what is really different is that the ability to do data mining, to do big data analysis, to actually process and use all the information, I think that is really what is changing, not so much what is being collected but the ability of companies to process and to use it.

Now, that said, I mean, we are getting ever more, because of people being connected with cell phones, people being on, you know, various social networks. But as I say, the information is out there.

How it is used? It is used in a lot of different ways. That is certainly something that is changing and evolving. But as I say, it is going to be increasingly used to target marketing messages and deals and special offers that are personalized to the consumer.

In terms of consumers' control over it, I am all in favor certainly of having a legal framework that gives consumers the ability to take control if they want to. I suspect that most consumers are not going to want to take control and that what we will see, which I think we have a history of in the United States, is consumers voicing a lot of concerns about privacy, but then when they learn that they can get, you know, 10 cents off on a Big Mac if they give up their privacy, they will give it up.

So I think it is a challenging issue. We can give consumers a lot of tools to protect the information. I am rather pessimistic whether consumers will make use of those tools.

Chairman JOHNSON. Mr. Brown and Ms. Hughes, what protections do consumers have if fraudulent, unauthorized, or inaccurate mobile payments are made to their account? What types of disclosures do consumers receive about risks associated with fraud and theft and the protections they have? Mr. Brown, let us start with you.

Mr. BROWN. This is another question that can be complicated based on the different archetypes for executing these transactions. If we take the two examples that I gave before—and there is actually a third where the transfer is more like a remittance, but I am just going to exclude that and talk about the prepaid wallet and the sort of credentialing Google Wallet-type structure.

With the mobile wallet on the Google model, where it is just a credentialing device, the protections and the disclosures that the consumer receives are those that are associated with whatever payment device the consumer has loaded into the wallet. I have a credit card here, so Reg Z would apply. If it is a debit card, Reg E would apply. Consumers Union has identified some real border cases where there is some question as to whether the particular instrument would be covered, but those I would characterize as real edge cases.

When you move into a mobile wallet—a stored-value-type product—the way I tend to think of it, and the way most of the providers of those services disclose the consumer protection, is that the wallet itself is covered by Reg E. That means that if I use my mobile wallet that is then backed up by a backup funding source and I end up in a dispute with the recipient of the transaction, that the transfer from my account to the recipient's account—Dwolla operates a system along these lines—would be protected by Reg E.

Typically, if you look at the terms of service associated with the providers of services like this—Dwolla is one, PayPal is another—you will see an outline of the protections that the consumer receives. Bill-to-mobile services raise some additional issues, and bill-to-mobile services on the whole generally disclose to consumers what the risks are. But there are some questions as to whether the coverage originates under the EFTA or the Truth in Billing Act and some additional State laws. So that is a short answer.

Chairman JOHNSON. Ms. Hughes, do you have anything to add?

Ms. HUGHES. Well, I would certainly agree with Mr. Brown that there are sufficient protections under Reg Z and Reg E right now. I think there may be some confusion to resolve through education with consumers about which of those are applying to which transactions. That is a big issue in my mind. And I do also agree with him that bill-to-mobile, which is basically both a matter of contract and a matter of the Truth in Billing Act, may add a layer of confusion to consumers that needs to be addressed through consumer education. I think this whole area could benefit from consumer education.

But I do think that we want to ensure that there are adequate and readily available and easily understood means for addressing payment alteration. That is what I said when I talked about pay-

ment data integrity, the possibility of a replication of a payment, that is, somebody who makes the payment more than once with only one authorization for the purpose. And, in addition, oddly enough, and the further the consumer is away from the merchant, the possibility of misdirecting a payment is an issue that is going to come up. Somehow I am going to misdial that phone number. I guarantee you I am going to misdial that phone number, but that is a different problem.

So I think that there are areas where additional work would be helpful. I think that instead of additional disclosures at this point, I would favor very enhanced education, but I would be willing to assist if disclosures come up in framing what I think would be appropriate disclosures.

Mr. BROWN. Can I add to that?

Chairman JOHNSON. Yes.

Mr. BROWN. I think Professor Hughes makes an important point that I want to amplify with respect to disclosures. I think when we talk about disclosures, we are maybe talking about two different things at the same time, and it is helpful to separate them.

On the one hand, there is information that is available about services. In some ways, that is what I think of as the disclosure. Consumers, by and large, are not the audience for that information. They tend not to page through the long terms of service associated with these services. That is information that academics, the FTC, and researchers make use of. Consumer Reports can evaluate different services and provide and educate consumers about which ones might be better and which ones are worse.

There is a separate issue about what gets communicated to consumers and when, and I think when we merge these two issues, we lose something, because I think a lot of times consumers are not particularly interested in getting long disclosures at the point that they are deciding to sign up for the service. They are deciding to sign up for the service because they want to complete some transaction—they want to do something. And reading a long disclosure is just not part of what they are excited about in wanting to complete that transaction.

So I think we should be careful to distinguish these two points, so maybe thinking about what information people should make available publicly about dispute rights versus what information needs to be disclosed to the consumer when they are signing up for the transaction or when they are engaging in a particular transaction.

Chairman JOHNSON. One last question relative to information security for the entire panel. Some experts claim that mobile payments are more secure than traditional payments while others claim that they pose additional threats to consumer safety and privacy. In your opinion, which side is right? Or are both sides right? Mr. Katz, let us begin with you.

Mr. KATZ. I guess being an academic contrarian, maybe I would say both sides are wrong.

[Laughter.]

Mr. KATZ. What I mean by that actually is the following: I think a lot of the debates are actually not about mobile, even though people act as if they are. So one of the things proponents of mobile

being more secure—one of the points they will make is, well, we can have two factor identification and we can use biometrics. Well, actually, as I understand it, the best way to do biometrics is not to use somebody's cell phone. The best way to do it is to have the customer either say here is who I am or use a phone or use a traditional payment card, just something to say here is who I claim I am, and then have the merchant access the data base to check what biometric information the customer should then provide, and the merchant to have the equipment that—you know, let us do retinal scans. The merchant should control the retinal scan. Why should I trust somebody's iPhone if he comes in and says, oh, yeah, I just did a retinal scan on Mike Katz, he is Mike Katz. I mean, the merchant is going to want to use its own equipment.

So I think all this stuff about biometrics which I often hear associated with mobile really is not about mobile. And I think there is a lot of that that goes on.

I think the answer is that we could make the systems a lot more secure than they are, but it is a question—in both mobile and traditional payments, and it is really a question of cost, and the industry has made the judgment to date that it is cheaper to deal with the fraud that occurs and just, you know, bear that than to try to have systems that are harder to tamper with.

Now, that said, I think that at least initially we are going to see the mobile systems are going to be less secure. And in terms of something about privacy, I noticed on the Web site of a company whose name I will not mention, but there were products that featured prominently in this hearing today, that company, it turns out—when you sign up with them, if you pay and you use this great service where you can pay using a merchant's mobile phone, if the merchant types the merchant's email address into the mobile phone, when you pay, anything you do in the future, the receipt goes to the merchant, not you. So, for example, if you pay your taxi driver and your taxi driver types his address into the mobile phone when you pay, the next time you go to the supermarket or something and use that service, the receipt goes to the taxi driver. That is not high-quality privacy. That is not something that has to be inherent in a mobile system, but it is something we see in the one.

And so I think what we are going to see is the following: I think what is really exciting about mobile and what is going on is it is bringing new players in the industry who are bringing in various forms of innovation, a lot of which has nothing to do with the mobile stuff. So with Square, coming in and charging lower fees to merchants, that is not because of the mobile part. It is because they have decided to aggregate small businesses' business and then go to Visa and MasterCard and get a lower rate. Basically, they have engaged in merchant service fee arbitrage.

Now, is it a coincidence that Square is doing that at the same time that they are bringing out this new innovative payment reader? I think, no, it is not a coincidence. The technology let a new company come in with new ideas, but a lot of the new ideas people are bringing in are not really about mobile.

So what I would say is that the technology has created opportunities, it is bringing in new players, those new players are then bringing in a whole lot of new ideas and innovations, often which

are not really tied to mobile. So it is a great thing, but I think we want to be careful about tying too much of that to mobile. I would say that even with the underbanked. I mean, I think—I do not understand actually what mobile does for the underbanked that you could not do already beyond—and I understand this is how the underbanked do use mobile, that they can check real-time balances all the time. But, of course, I can use—I could have a mobile app to check real-time balances even if I never made a mobile payment in my life.

So on all of these things, I think it is really important to separate out which part is mobile and which part is innovation, because if we try and tie them too much together, it just may give us the wrong perspective.

I should turn things over to my fellow panelists.

Chairman JOHNSON. Ms. Hughes, what do you think?

Ms. HUGHES. Well, I think Professor Katz has given us a very provocative possibility to imagine, and I am inclined to agree that many of these innovations have very little to do with mobile. They are just payments innovations or great arbitrage opportunities.

But I would make one simple point, and that is that the more people who have their hands on data based on the experience of the last few years in particular, the more opportunities there are for the introduction of malware or interception of payment data. As I mentioned earlier, the banking industry is quite concerned about this and about possibly weak incentives for some of these people who are not quite at the merchant and not quite at the bank not to have strong enough protections in their own systems.

When we have events such as happened with Global Payments not so long ago, a processor, we realize that the more people that have hands, the more problems could happen. Now, that is not unique to mobile. The thing that might be unique to mobile is an enhancement of the number of players in any particular payment transaction. That could be problematic.

Chairman JOHNSON. Mr. Brown.

Mr. BROWN. I guess I will play the contrarian and be a little optimistic on this point. Although I think it is possible to identify some potential downsides, as Professor Katz and Professor Hughes have done on the information security issue, I think it is also important to recognize that the transition from traditional form factors for payments to mobile and the emergence of some of these new technologies that mash up payment functions with other commercial functions introduce both new data that people can analyze to produce better outcomes with respect to risk and fraud and, second, make it easier to introduce dynamic data into the payment infrastructure.

The issue that creates the risk associated with credit card fraud is that the data on the card, both the physical manifestation and what is visible on the mag stripe, is static, not dynamic. So once it is obtained, it can be used in some circumstances to generate a transaction at another merchant. That is an issue with how the data currently resides.

When we make the transition to a mobile device, we have the opportunity to introduce dynamic information, and we can do it in a way that is easier. As Professor Katz would point out, if we are

really concerned about dynamic data, can't we do it with mag stripes? And the answer is yes, though no one is. This inflection point provides an opportunity to introduce new data that has the potential to make retail payments even more secure than they already are, which, frankly, if you look at the reported fraud numbers on the major payment card systems, is pretty remarkably secure under the existing infrastructure.

Chairman JOHNSON. I would like to thank our witnesses for their very interesting testimony.

The Committee will continue its series of hearings on the development and adoption of mobile payments in the fall.

This hearing is adjourned.

[Whereupon, at 11:04 a.m., the hearing was adjourned.]

[Prepared statements supplied for the record follow:]

**PREPARED STATEMENT OF MICHAEL L. KATZ**

SARIN CHAIR IN STRATEGY AND LEADERSHIP, PROFESSOR OF ECONOMICS, UNIVERSITY OF CALIFORNIA, BERKELEY

JULY 10, 2012

Chairman Johnson, Ranking Member Shelby, and Members of the Committee, thank you for inviting me to appear before you today to talk about mobile payments.

America's consumers are increasingly connected via smart phones, tablet computers, and other mobile devices. Many people have predicted that the use of near-field communications (or NFC), a technology which allows consumers to pay by swiping their phones rather than their credit or debit cards, will revolutionize consumer payments at bricks-and-mortar merchants. I disagree. I believe the changes associated with NFC and so-called digital wallets will be evolutionary, not revolutionary. There will be a revolution resulting from the ubiquity of smart phones and tablets, but that revolution will manifest itself in the ways merchants manage their relationships with their customers.

Today, merchants and consumers already have access to a wide range of payment options, including cash, checks, and various payment cards. These options are easy to use, widely accepted, and trusted. Moreover, most consumers already have established relationships with payment service providers, and merchants have made significant investments in equipment, systems, and employee training to utilize these payment services. In order for new payment services based on smart phones and tablets to compete successfully, these services will have to offer merchants and consumers additional value in comparison with current options. Cool technology alone will not be enough.

Merchants will be attracted to mobile payments if those services either lower the merchants' costs of completing transactions or attract additional consumer patronage. How will mobile payment services attract customers to bricks-and-mortar merchants? Surveys demonstrate that consumers want payment services that are widely accepted, easy to use, and trustworthy. So how do mobile payments stack up against the competition?

When it comes to paying at bricks-and-mortar merchants, the extent of acceptance is a weakness, rather than strength. Indeed, mobile payment services face a chicken-and-egg problem. Specifically, a merchant does not want to bear the expense of changing its checkout process to accommodate a new payment service if there are few consumers who use that service. Similarly, a consumer does not want to sign up for the payment service if there are few merchants who accept it. But if everyone waits for everyone else to join first, the new service will never get off the ground. There are several potential solutions to the chicken-and-egg problem but all of them rely on a common underlying factor: there has to be some source of benefit that makes it worthwhile to invest in overcoming the chicken-and-egg problem. So we are back to looking for the source of consumer value.

An NFC-enabled digital wallet can be more convenient and possibly easier to use than a conventional wallet filled with multiple payment cards. It is worth observing, however, that most of us are going to have to carry conventional wallets anyway, at least until drivers' licenses and insurance cards and the like also go digital. Moreover, is it really that much easier to swipe your phone than a smart card? In the short run, ease-of-use benefits appear to be too limited to be a significant driver of adoption.

That leaves trust as a source of value. Security and privacy are two critical elements of trust. Consumer surveys reveal that many consumers question the security of mobile payments, and indeed mobile payment systems do have points of vulnerability, such as the radio interface, that card-based systems do not. Moreover, through the use of malicious code downloaded through apps or Web browsing, a smart phone can be compromised without the attacker's having to attain physical proximity. Consequently, security is not going to be a positive driver of mobile payment adoption any time soon. Things do not look more promising in terms of privacy. Consumer surveys reveal that many consumers worry that mobile payment companies will collect too much personal information and that that information will be misused.

If ubiquity, ease of use, and trust all create too little value to drive widespread adoption of mobile payments, what will? I believe the answer lies in the very information that consumers worry will be misused. The widespread adoption of smart phones and other mobile devices with increasing capabilities has made it possible to collect detailed data about where consumers are and what they are doing. This information can be analyzed to predict consumer behavior and used to generate personalized, context-specific, merchant-to-consumer communication delivered in real

time. The ability to predict consumer behavior and send such targeted messages is a very powerful marketing tool that will be worth tens of billions of dollars annually to merchants.

A hypothetical example illustrates some of the possibilities. A mobile payment app might alert a coffee retailer at 10:45 a.m. that a person who on most days purchases a cup of coffee by 10:30 is just leaving her office and has yet to visit a coffee shop today. Taking into account the summer heat and the fact that the retailer is not very crowded right now, the retailer could send an email or text message to the consumer offering a 20 percent discount on an iced coffee if she comes into the store three blocks away in the next 30 minutes. In summary, information and communication lie at the heart of the coming mobile payment revolution.

Mobile payments represent the convergence of three industries: telecommunications, banking, and Web services. This industry convergence is going to lead to complex regulatory convergence as well. The interplay of economy-wide antitrust policy and privacy regulation with the sector-specific regulatory regimes for banking and telecommunications is going to be problematical for the industry. It may also confuse consumers and give them false senses of security and/or risk. However, properly implemented, regulation could foster well-placed consumer trust and, thus, promote the adoption of mobile payments. Given the importance of information and the complexity of the issues involved in regulating the collection and handling of it, public policy concerns regarding privacy will loom large for years to come.

Thank you again for inviting me to appear before you today. I would be happy to answer any questions you might have.

**INCREASING CONNECTEDNESS AND CONSUMER PAYMENTS:  
AN OVERVIEW**

**Michael L. Katz\***

**1 May 2012**

\* This paper was commissioned by the Federal Reserve Bank of Kansas City. Two discussants, Don Kingsborough and Hal Varian, provided helpful comments on an early draft. I gratefully acknowledge Nokia Corporation's financial support for Berkeley's Program in Business Model Innovation.

## CONTENTS

<b>I.</b>	<b>INTRODUCTION AND OVERVIEW</b> .....	<b>1</b>
<b>II.</b>	<b>DOES ANYONE WANT MOBILE PAYMENTS (OTHER THAN MOBILE PAYMENT PROVIDERS)?</b> .....	<b>6</b>
A.	WHAT DO USERS WANT FROM PAYMENT PRODUCTS?.....	7
1.	<i>Merchants' Desiderata</i> .....	7
2.	<i>Consumers' Desiderata</i> .....	8
B.	WILL INCREASING CONNECTEDNESS ENABLE PAYMENT SERVICES THAT BETTER SATISFY USER DESIRES?.....	12
1.	<i>Merchant Perspective</i> .....	13
2.	<i>Consumer Perspective</i> .....	14
<b>III.</b>	<b>IT'S ALL ABOUT THE BENJAMINS, AND THE BENJAMINS ARE ALL ABOUT THE INFORMATION</b> .....	<b>22</b>
A.	I SAW WHAT YOU DID, I KNOW WHO YOU ARE.....	22
B.	SEARCHING NEAR OR FAR FOR A VALUE PROPOSITION.....	25
C.	WHO WILL CONTROL CONSUMER INFORMATION?.....	28
D.	REGULATION, REGULATION, REGULATION.....	31
<b>IV.</b>	<b>GETTING FROM HERE TO THERE</b> .....	<b>33</b>
A.	CONSUMER TRUST.....	34
B.	NETWORK EFFECTS AND THE CHICKEN-AND-EGG PROBLEM.....	35
<b>V.</b>	<b>WHO WILL DO WHAT?</b> .....	<b>41</b>
A.	DON'T GET CARRIED AWAY WITH CARRIERS.....	41
B.	GIVE BANKS CREDIT.....	46
C.	WITHER INCUMBENT PAYMENT CARD NETWORKS?.....	48
D.	WEB-SERVICES COMPANIES.....	48
E.	WHAT ABOUT APPLE?.....	49
<b>VI.</b>	<b>CONCLUSION</b> .....	<b>51</b>

**I. INTRODUCTION AND OVERVIEW**

1. This paper presents a view of the future consumer payments. Specifically, I opine on two questions. First, will the broad trends of consumers' increasingly being connected via mobile access devices and engaging in social networking be likely to revolutionize consumer payments? Second, if so, what roles will be played by the various payment participants (*e.g.*, consumers, merchants, banks, mobile network operators, and nonbank intermediaries)?

2. This is a rather daunting task. Fortunately (for me, at least) confidently making sweeping predictions that fail to materialize is something of a mobile payments industry tradition. In that spirit, I will use the occasion to make my own sweeping and, possibly, far-fetched predictions.

3. In short, I believe that, in the United States and other advanced economies, the ubiquity of always-connected individuals with access to computing power, coupled with the near-total loss of privacy due to social and technological factors, will lead to evolutionary developments in core payment services but revolutionary changes in services that are built on the information collected through payment services.<sup>1</sup> Moreover, I think that core payment services will become only one component of broader constellations of services that: (a) provide consumers an integrated user experience when dealing with merchants, and (b) provide merchants with customer relationship management and marketing services, in addition to payment services.

---

<sup>1</sup> Throughout, when talking about either fixed or mobile access devices, I will be agnostic as to whether the computing power lies in access device itself or the cloud.

4. The evolutionary changes in payments will come in the form of additional payment options that largely are extensions of existing payment options (*e.g.*, the extension of credit card networks to mobile-commerce transactions, and the use of smart phones as smarter smart cards through the use of near field communication (NFC)). In the short term, we may see new mobile payment products that are complementary to, and offered separately from, existing payment products. In the long term, I predict that successful payment products will provide consumers the convenience of one-stop shopping. That is, these payment mechanisms will be useful for mobile commerce, e-commerce, and traditional bricks-and-mortar commerce, and they will be so whether the consumer is buying virtual or tangible goods and services. Widely useable payment services will also have the advantage of allowing the service providers to collect more comprehensive information about any given consumer.

5. I believe this latter advantage will be an important one because the revolutionary services building on mobile, connected computing and social networking will be those services that allow merchants to target their customers based on the information collected through payment and social networks. Both of the trends identified in the opening of this essay will help incite revolution. First, connected individuals can be identified and tracked so that detailed information about their environment and actions can be collected, analyzed, and used to generate personalized, context-specific communication that can be delivered in real time. Second, social networks can allow the identification of an individual's revealed preferences, demographic characteristics, sources of influence, and influencer value. The ability to predict consumer behavior, know the consumer's context, and send personalized

messages can give merchants very powerful marketing tools, worth tens of billions of dollars annually.<sup>2</sup>

6. Technological and social trends will lead to the convergence of three sectors around payment systems: telecommunications, banking, and web services. The communications sector will provide fixed and mobile Internet access services that will serve as bases on which innovative services will be built. Entities in the banking sector will extend credit and provide trusted brands. Lastly, a wide range of firms from the web-service sector may be involved, with particularly important roles played by social-networking, search, and online-advertising providers.

7. Any given mobile payment service requires the tacit or explicit cooperation of a wide range of parties to succeed, including mobile operating system (OS) providers, app developers, mobile access device original equipment manufacturers (OEMs), wireless telecommunications carriers, financial institutions (*e.g.*, credit-issuing banks and merchant-acquiring banks), payment network operators, and possibly others. All of these parties are also potential rivals seeking to appropriate profits for themselves. Hence, although these parties must cooperate with one another to create value, they compete to capture that value. Similar forces arise with respect to the customer-relationship-management and targeted-marketing services that are based on the data collected through payment services and social networks.

---

<sup>2</sup> As discussed below, the increased understanding of consumer behavior may also have benefits for payment products themselves in terms of improved customization of credit terms and more-effective fraud detection and control.

8. The battles to capture value will occur on several fronts. First, there may be standards wars and compatibility battles. I believe that merchant demand for standardization of point-of-sale (POS) transaction-capture devices will lead to the standardization of those devices, but that these devices will be flexible enough to interact with consumer devices in a variety of ways. Second, there will be struggles to control the customer relationship. However, I do not expect there to be one firm or one type of firm that controls “the” customer relationship in this area. Rather, a given consumer may have business relationships with several members of the relevant value net simultaneously.

9. The most important battles for control will be over information ownership. Revolutionary services will be based on the unprecedented amounts of information collected about consumers, and this information will be extremely valuable. Many firms will adopt business models predicated on monetizing the information that they collect about their users. Consequently, there will be struggles among social networks, other app providers, payment network operators, mobile network operators, and even mobile access device OEMs (at least in the case of Apple, Inc.) over the ownership and control of this information. In the U.S., regulatory and political pressures will have significant influences on industry evolution and who captures value. The convergence of three different sectors is going to lead to complex regulatory convergence as well. The interplay of economy-wide competition policy and privacy regulation with the sector-specific regulatory regimes for banking and telecommunications is going to be problematical for the industry. Given the importance of information and the complexity of the issues involved in regulating the collection and handling of it, public-policy concerns regarding privacy will loom large for years to come.

10. An examination of the broad forces affecting the industry gives rise to several specific predictions about the roles likely to be played by various industry participants:

- *The roles of firms in the telecommunications sector will change little.* With the possible exception of Apple, Inc., I do not see wireless telecommunications carriers and mobile access device OEMs playing significant roles in mobile payments beyond offering generic infrastructure on which payments services offered by other providers ride.
- *The roles of banks will change little.* Banks will continue to be an important part of the payment ecosystem as providers of credit, for which they possess unique expertise based on extensive experience. In addition, in the light of consumer concerns about privacy and security, banks may play an important role in reassuring consumers of the integrity of mobile payment systems.
- *Current payment card networks will play a central role if they can successfully innovate.* Traditional payment card networks, such as American Express, MasterCard, Visa, and—to a lesser extent—Discover have powerful competitive advantages in form of trusted brands and large networks of consumers and merchant users. A critical question is whether they possess the organizational capabilities to innovate to take advantage of the new possibilities created by pervasive consumer connectedness.
- *Web services firms will play significant roles as information collectors and processors.* Web services firms, such as Amazon, Facebook, and Google, are largely information collection-and-processing companies. To varying degrees, these companies have valuable competitive assets that include massive amounts of

consumer data and the ability efficiently to collect, store, and analyze those data to model consumer behavior. Given these assets, I expect a few of these firms to be very successful in this area.

11. The remainder of this paper is organized as follows. Section II examines whether consumers and merchants are likely to derive significant new benefits from the types of payment services and features enabled by increasing consumer connectedness. The presence or absence of such benefits will have a significant impact on the likelihood that mobile payments and social-network-based payment services are likely to be widely adopted. Section III discusses the potential uses of the consumer information that would be collected by these payment services. It also discusses the likely struggle for control of that information. Section IV then discusses some of the possible reasons why these payment services have not been widely adopted to date, and it identifies some of the strategies that may overcome these barriers to adoption. These first three substantive sections set the stage for Section V to offer a predictive analysis of the likely winners and losers among the various types of firms that will be involved in providing new payment services. A very brief summary section closes the paper.

## **II. DOES ANYONE WANT MOBILE PAYMENTS (OTHER THAN MOBILE PAYMENT PROVIDERS)?**

12. “Mobile” payment services already are offered by cash, checks, and various payment cards. These payment instruments are light-weight, compact, widely accepted, and easy to use. Rightly or wrongly, American consumers are also very comfortable with these payment instruments with respect to privacy and security. Moreover, most consumers already have established relationships with payment service providers, and merchants have made

significant investments in POS transaction-capture devices (*e.g.*, card readers and cash registers), employee training, and supporting information technology systems to utilize these payment instruments. These facts raise the question: do merchants and consumers want new payment options based on mobile access devices and/or social networks? The answer to this question is important because, if merchants and consumers do not see value in a new payment service, then that service is very unlikely to succeed. Cool technology alone is not enough.

**A. WHAT DO USERS WANT FROM PAYMENT PRODUCTS?**

13. New payment services will be successful only if they offer merchants and consumers additional value sufficient to induce them to change payment methods or service providers.

What are the sources of value to these users?

**1. Merchants' Desiderata**

14. Logically, the ideal payment service from a merchant's perspective is one that imposes low costs on the merchant and is used by a large number of consumers to make purchases in high volumes. And, indeed, in their empirical examination of merchant behavior with respect to mobile payment services, Mallat and Tuunainen (2008) found "that the main adoption drivers are related to the means of increasing sales or reducing the costs of payment processing".<sup>3</sup>

15. Merchants care about the complete set of costs that they incur to utilize a payment service. These costs include: (a) the fees, if any, charged by the payment service provider (*e.g.*, the merchant discounts charged by a credit card network); (b) expenditures on activities

---

<sup>3</sup> Niina Mallat and Virpi Kristina Tuunainen (2008) "Exploring Merchant Adoption of Mobile Payment Systems: An Empirical Study," *e-Service Journal* 6(2): 24-57 (hereinafter, Mallat and Tuunainen (2008)) at 24.

that must be undertaken by the merchant to utilize the payment service (*e.g.*, employee training and the wages and real-estate costs associated with using the payment service at check out); (c) payments to third-parties for activities related to using the payment service; and (d) costs incurred to detect and prevent fraud by consumers, the merchant's employees, or other members of the relevant payment service value net.

16. Most merchants feel the need to accept payment services that consumers would like to use. Hence, merchant demand for payment services is derived in large part from consumer demand. Indirectly at least, merchants want what consumers want. In general, a merchant will be especially interested in a payment instrument that allows the merchant to attract customers who would not patronize the merchant absent the ability to utilize that payment service. Indeed, a rational merchant will accept a high-cost payment service if doing so allows the merchant to attract customers who would otherwise not patronize it.

## 2. Consumers' Desiderata

17. Because merchant demands are largely derived from consumer demands, it is particularly important to understand what consumers want from a payment service and whether they are likely to adopt mobile payment solutions.<sup>4</sup> The research literature has identified several factors that influence consumer demand for mobile payments. In their survey of American consumers, Dewan and Chen (2005) interpreted the results as suggesting "that consumers realize the potential benefits (*e.g.* improved transaction speed and convenience) of mPayment, but at the same time, consumers are expressing grave security

---

<sup>4</sup> For purposes of this paper, it is sufficient to examine the drivers of consumer adoption at a broad level. In practice, consumer payment decisions are typically made at the transaction level, and the choice of payment instrument can vary with consumer characteristics, transaction characteristics, and payment-service characteristics.

and privacy concerns.”<sup>5</sup> Based on their survey of New Zealanders, Viehland and Leong (2007) found that convenience was a key reason for consumers to choose mobile payments, while being less convenient than cash, and concerns about security—particularly confidentiality—were prominent barriers to adoption.<sup>6</sup> In addition, the authors found that an aversion to paying service fees was the single reason most often stated for no using mobile payments.<sup>7</sup> In a more recent study, Andreev *et al.* (2011) found “empirical evidence that trust, willingness to transact, and perceived ease of use are key factors in explaining [a] consumer’s willingness to make an m-payment, with trust having the largest explanatory power.”<sup>8</sup>

18. It is useful to examine several different dimensions of consumer preferences in turn.

19. *Convenience and ease of use:* It seems to be intuitively clear that consumers want mobile payments to be quick, easy, and not require a lot of knowledge specific to a particular payment service. However, Andreev *et al.* (2011, p. 122) found

that while causation exists between perceived ease of use and willingness to make an m-payment, the association is relatively weak. This illustrates that perceived ease of use of the technology is not a

---

<sup>5</sup> Sunil Dewan and Lei-da Chen (2005) “Mobile Payment Adoption in the US: A Cross-Industry, Cross-Platform Solution,” *Journal of Information Privacy and Security*, 1(2): 4-28, available at [http://www.sunildewan.com/uploads/mpayment\\_Journal\\_of\\_Information\\_Privacy\\_and\\_Security.pdf](http://www.sunildewan.com/uploads/mpayment_Journal_of_Information_Privacy_and_Security.pdf), site visited April 23, 2012 (hereinafter, Dewan and Chen (2005)), at 23. Page cites made to this document correspond to the version available at URL above.

<sup>6</sup> Dennis Viehland and Roslyn Siu Yoong Leong (2007) “Acceptance and Use of Mobile Payments,” *ACIS 2007 Proceedings*, Paper 16, Tables 4 and 5.

<sup>7</sup> *Id.*, Table 5.

<sup>8</sup> Pavel Andreev, Aidan Duane, Philip O’Reilly (2011) “Conceptualizing Consumer Perceptions of Making M-Payments Using Smart Phones in Ireland,” in *Researching the Future in Information Systems*, Chiasson, Henfridsson, Karsten, and DeGross (ed.s). Springer: Boston (hereinafter Andreev *et al.* (2011)) at 122.

key determinant of consumers' willingness to make an m-payment using a smart phone.

Similarly, Schierz *et al.* (2010) found that perceived ease of use was much less important for intention to use than was "perceived compatibility," where perceived compatibility was measured by the answers to questions regarding whether the respondent agreed that mobile payment services fit well with his or her lifestyle and the way in which he or she likes to purchase products and services.<sup>9</sup>

20. *Ubiquity*: Consumers generally want a payment instrument that they can use to make payments at their preferred merchants. Hence, all else equal, the greater the number and variety of merchants accepting a given payment service, the more attractive one would expect that service to be to consumers. Although he is careful not to assert that he has established causation, in his empirical study of credit card usage, Marc Rysman (2007) found that a consumer's choice of card network as his or her favorite is positively correlated with the degree of local merchant acceptance of that network, which suggests a positive feedback loop between merchant card acceptance and consumer card usage.<sup>10</sup>

---

<sup>9</sup> The correlation between perceived compatibility and perceived ease of use was only 0.25. (Paul Gerhardt Schierz, Oliver Schilke, and Bernd W. Wirtz (2010) "Understanding consumer acceptance of mobile payment services: An empirical analysis," *Electronic Commerce Research and Applications*, 9(3): 209-216 at 215.)

Other authors have also examined the effects of compatibility on adoption. Because of its somewhat amorphous nature, I do not discuss it further in the present paper, except to note two points. First, because consumers' notions of compatibility can vary by transaction type (*e.g.*, quick service restaurant purchases versus major appliance purchases), these notions can have important effects on the types of transactions for which consumers will use mobile payments. Second, I fully expect the population of users obsessed with their iPhones to find any Apple mobile payment service to be compatible with their lifestyles.

<sup>10</sup> Marc Rysman (2007) "An Empirical Analysis of Payment Card Usage," *The Journal of Industrial Economics*, 55(1): 1-36.

21. *Security and privacy:* As noted above, studies have found that consumers are reluctant to use payment services that they do not trust. Similarly, Mallat (2007) found that consumers were more willing to transact with trustworthy parties.<sup>11</sup> Security and privacy are two critical elements of trust.<sup>12</sup>

22. *Credit:* At the start of 2012, American consumers had approximately 800 billion dollars of revolving-credit debt.<sup>13</sup> Manifestly, many American consumers desire the provision of credit by some—although by no means all—payment services.

23. *Rewards:* Many consumers are more willing to use a payment service if they are paid to do so.<sup>14</sup> Indeed, regulators in several nations (most notably, Australia) have expressed concern that credit-card rewards programs have led to consumers' using credit cards to a greater extent than is efficient. The use of rewards programs to motivate consumer use of mobile payment services may be a particularly important factor if it turns out that these services do not offer significant additional value for consumers but do generate significant benefits for merchants or for payment service providers in some other way (*e.g.*, the monetization of the information they collect about consumer behavior).

---

<sup>11</sup> Niina Mallat (2007) "Exploring consumer adoption of mobile payments – A qualitative study," *Journal of Strategic Information Systems*, 16: 413–432 (hereinafter, Mallat (2007) at 424.

<sup>12</sup> For example, Andreev *et al.* (2011, p. 123) found that "that consumer's [sic] perceptions of the privacy controls employed by smart phone service providers is [sic] a critical element of trust."

<sup>13</sup> Federal Reserve Bank, *Consumer Credit - G.19*, released April 6, 2012, available at <http://www.federalreserve.gov/releases/g19/current/default.htm>, site visited April 27, 2012.

<sup>14</sup> See Andrew Ching and Fumiko Hayashi (2010) "Payment card rewards programs and consumer payment choice," *Journal of Banking & Finance*, 34(8): 1773-1787, and the references cited therein for empirical estimates of the sensitivity of consumers' choices of payment instruments to the presence of reward programs.

24. *Account management tools*: Clearly, consumers desire the ability to monitor their accounts to at least some degree in order to check their balances, review the transactions charged against their accounts, and keep tabs on the finance charges levied on them.

**B. WILL INCREASING CONNECTEDNESS ENABLE PAYMENT SERVICES THAT BETTER SATISFY USER DESIRES?**

25. What difference does it make for payment services that consumers are increasingly connected through mobile access devices and social networks? Consider first the effects of pervasive social networking. I, at least, lack the imagination to see social networking having a huge influence on payment services narrowly defined. One could imagine embedding a payment service within a social network to facilitate online shopping or to transfer money among friends, but this strikes me as being a modest extension of the scope of existing services rather than a breakthrough new service.

26. Turning to connectedness through mobile access devices, the widespread adoption of smart phones and wireless tablets gives rise to several capabilities, including:<sup>15</sup>

- Consumers almost always have the ability to establish two-way communication links with merchants and/or payment networks.
- Consumers almost always have memory and processing power easily accessible to them.
- Consumers almost always have sensors with them, which may detect and report information such as location and temperature, or capture video images.<sup>16</sup>

---

<sup>15</sup> Although tablets are generally more capable than smart phones, consumers are less likely to have tablets with them and readily accessible at all times. Hence, tablets may be the preferred means of engaging in e-commerce transactions at home but smart phones will be used while at bricks-and-mortar retailers.

27. In order to predict whether these capabilities will enable successful new payment services, one must examine if and how these capabilities enhance the ability of payment services to offer value to consumers and merchants.

#### 1. Merchant Perspective

28. As discussed above, merchants will value payment services that make use of increasing consumer connectedness if those services either lower merchants' costs of completing existing transactions or attract additional consumer patronage.

29. Mobile payment services might lower merchants' costs by charging lower fees than current services. In theory, lower fees could arise because: (a) mobile infrastructure is less costly than existing infrastructure, which seems unlikely in practice; (b) other features of mobile payments facilitate new entry, which leads to increased competition in the provision of payment services; or (c) mobile payments services have other revenue streams (*e.g.*, the sale of consumer information), which create incentives to charge lower prices to merchants and consumers in order to generate additional use. Mobile payment services might also lower merchants' costs in other ways, such as reducing the length of time it takes a consumer to check out of a store or restaurant.<sup>17</sup> For example, Starbucks offers a mobile app to its customers that draws funds from Starbucks prepaid loyalty-card accounts and generates two-

---

<sup>16</sup> I will not discuss them further, but it is worth noting in passing that there are also new features and services enabled by the form factors of mobile access devices compared to traditional payment cards. Even the smartest smart card cannot change its look and logo in real time. But a smart phone or tablet can. This fact opens new possibilities for co-branding. For example, a mobile payment account might be co-branded with petroleum company when used to buy gas and a department store when used to purchase clothing.

<sup>17</sup> There might be potential cost savings for very small merchants from using smart phones or tablets as their primary point-of-sale, transaction-capture devices (one of Square's principal services offers these benefits, among others).

dimensional barcodes that customers can use to pay for purchases by having the codes scanned at the point of sale. The president of Starbucks' U.S. operations stated that a primary benefit of the application is the ability to speed up the checkout process.<sup>18</sup>

30. In terms of attracting additional customers, mobile payment services clearly are valuable to merchants that rely on online shopping channels; many consumers do online commerce via smartphones and, especially, tablets. Mobile payment services will also be valuable to merchants if there are other reasons that consumers value using mobile payment services even when not engaging in online shopping.

## 2. Consumer Perspective

31. So why would a consumer want to use a mobile phone or other wireless access device to pay for something? Consider how the new capabilities identified above affect the ability to satisfy the consumer wants identified above:

32. *Ubiquity:* At least initially, mobile payment services might serve as complements to traditional payment services by extending the reach of their merchant acceptance networks. E-commerce transactions require Internet access. Many people's first choice for an Internet connection is their phone or tablet. This is especially likely to be true for consumers purchasing apps or content for their phones or who are traveling, but it is also true for many consumers ordering tangible goods online from home, such as when watching television in their living rooms.

---

<sup>18</sup> Kate Fitzgerald, "Starbucks National Push for Mobile Payments," *American Banker*, December 3, 2010, available at [http://www.americanbanker.com/issues/175\\_232/starbucks-mobile-payments-1029437-1.html](http://www.americanbanker.com/issues/175_232/starbucks-mobile-payments-1029437-1.html), site visited March 12, 2012.

33. *Convenience and Ease of Use:* Eventually, people may stop carrying wallets to hold cash and various identification cards, such as drivers' licenses and insurance cards. If all of this information were stored in a smart phone, then storing payment-service information there, too, would be a benefit. But in the short run, people will continue to carry traditional wallets. This fact raises the questions: How hard is it to swipe a traditional credit or debit card, and why is it better to swipe a smart phone than swipe a traditional wallet with a contactless smart card in it?

34. The only advantage I can see is the following. If you are one of those annoying people who talks on your mobile phone when you should be handing your credit card to the cashier, now the cashier can simply grab your phone, swipe it, and send you on your way. In other words, I don't see much of a benefit from swiping a phone instead of swiping a card. But then again, I am the sort of person who would rather talk to my dinner companion than spend my time in the restaurant checking in on Facebook to tell people I am having dinner.

35. There are services that go beyond being a smarter smart card and eliminate the need for even contactless swiping. For example, Square has a service that does not require the consumer to touch his or her phone or a payment card in order to be billed.<sup>19</sup> Such services are manifestly more convenient, but they raise issues of consumer trust. One can imagine it taking a long time for consumers to adopt this payment method anywhere other than merchants at which they shop regularly (*e.g.*, to get their morning coffee or quick-service lunch).

---

<sup>19</sup> <https://squareup.com/pay-with-square>, site visited April 20, 2012.

36. *Security and Privacy*: Consumers might be induced to use a mobile payment service if they thought it were more secure and/or offered greater privacy protections than other payment options. Existing studies, however, indicate that many consumers hold the opposite view. For example, Dewan and Chen (2005) found that over half of the consumers responding to their survey felt that mobile payment systems were either “not secure” or “not secure at all,” while just under half felt these systems posed either a “high risk” or “very high risk” to privacy.<sup>20</sup> The biggest concerns regarding security were whether the transactions would be properly authenticated and whether the data exchanged during the transactions would be available to unintended users.<sup>21</sup> In terms of privacy concerns, Dewan and Chen (2005) found that almost half of the consumers responding to their survey expressed concern about mobile payment companies’ collecting too much personal information; over a quarter of respondents were concerned that personal information in the companies’ databases would be used for purposes consumers had not authorized; and over a quarter of respondents were concerned that their personal information in the companies’ databases was not protected.<sup>22</sup> The consumers surveyed expressed much less concern about errors in the information contained in the databases.<sup>23</sup> More recently, a consumer survey conducted in late 2011 found

---

<sup>20</sup> Dewan and Chen (2005) at 14.

<sup>21</sup> *Id.* at 15 and 16.

<sup>22</sup> *Id.* at 17 and 18.

<sup>23</sup> *Id.*

that the vast majority of consumers considered their personal computers to be more secure means of online shopping than their mobile phones or tablets.<sup>24</sup>

37. Will technological developments make mobile payments more secure? Some observers credit mobile payment services with having authentication based on devices (*i.e.*, mobile phones) that are identified with particular individuals. But existing payment cards already possess this property. One might argue that mobile access devices are superior to payment cards as authentication tokens because the former can provide biometric authentication capabilities. However, those capabilities could more reliably be delivered by merchant-controlled POS devices that could check a consumer's claimed identity against a network database of biometric information.<sup>25</sup>

38. Although personal devices and biometrics do not distinguish mobile payment systems, consumers' having the ability to establish two-way communication links with merchants and/or payment networks does. Specifically, an always-connected buyer can direct payment to a merchant via communication with a payment network, without relying on the merchant's facilities.<sup>26</sup> This means that a consumer could communicate solely with a trusted partner

---

<sup>24</sup> Ann Carns, "Consumers Leery of Online Shopping with Tablets and Phones," *The New York Times*, January 27, 2012, available at <http://bucks.blogs.nytimes.com/2012/01/27/consumers-leery-of-online-shopping-with-tablets-and-phones/>, site visited April 30, 2012.

<sup>25</sup> The identity claim might be made by a consumer orally, by swiping his or her payment card, or by a message sent by his or her mobile phone to the merchant.

<sup>26</sup> With an NFC-based service, the consumer's mobile access device would still communicate with a POS terminal controlled by the merchant. But in other cases, such as the use of WiFi or traditional cellular services, the consumer's mobile access device could communicate with the payment network "directly." The Pay with Square service allows this to be done. (<https://squareup.com/pay-with-square>, site visited April 20, 2012.)

In contrast, Square's innovative mobile card reader reportedly can easily be used to skim credit card information. Square's defense is that all credit cards can be skimmed. ("Square

when dealing with potentially untrustworthy merchants. This makes the system much safer in terms of certain types of merchant fraud, such as card skimming. In addition, an always-connected consumer can be provided real-time fraud alerts and as well as the ability to engage in real-time tracking of transactions. For example, with Pay with Square, a consumer gets a notification on his or her mobile device confirming the payment.<sup>27</sup>

39. Mobile systems also have vulnerabilities. Overall, the use of wireless might well be expected to weaken security because there are more points of vulnerability (*e.g.*, the radio network) at which to hack a smart-phone-based system than a smart-card-based one.

Moreover, through the use of malicious code downloaded through apps or web browsing, a smart phone can be compromised without the attacker's having to attain physical proximity.

40. New payment services, mobile or otherwise, may have to make tradeoffs between ease of use and privacy. For example, in a message to merchants, Square states that<sup>28</sup>

[a]fter a customer elects to receive a receipt via email or text message, our system links the entered email address or phone number to their payment card. This way, the next time they pay with Square their information automatically populates, making the process much faster.

Because of this feature, if you happen to enter your own information for your customers' receipts, you'll receive their receipts any time they pay another Square user with the same card.

Although this process may be convenient, one cannot say that it provides state-of-the-art privacy.

---

answers VeriFone's accusations on security of mobile credit card reader," Los Angeles Times, March 10, 2011, available at <http://latimesblogs.latimes.com/technology/2011/03/square-answers-verifones-accusations-on-security-of-mobile-credit-card-reader.html>, site visited April 20, 2012.)

<sup>27</sup> <https://help.squareup.com/customer/portal/articles/108037-pay-with-square-where-can-i-find-my-receipts-and-payment-history->, site visited April 20, 2012.

<sup>28</sup> <https://help.squareup.com/customer/portal/articles/197741>, site visited April 12, 2012.

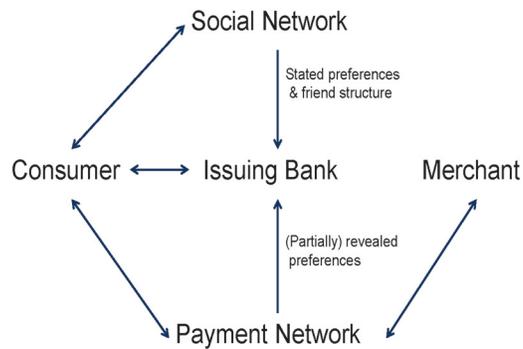
41. This example brings up a broader point. American consumers have a history of saying that they care deeply about privacy and security (especially with respect to new technologies) but then acting as if they care little. To the extent that mobile payments services are less trustworthy, consumers ultimately may not be troubled. And there may turn out to be limited demand for the additional security features that mobile payments systems can provide. For example, an e-commerce solution in which people handle payment transactions on a web page that is *not* accessed through the merchant's web page would be easy to create, yet to my knowledge consumers typically get to services such as those offered by PayPal by being redirected by the merchant's web site, and many customers are very comfortable with the security of those services.

42. *Credit.* Mobile payment services and social network generate information on a consumer's context and transaction histories. Figure 1 below presents a schematic view of important potential information flows.<sup>29</sup> As illustrated by the figure, this information could serve as additional input into credit scoring models (for example, if other members of your social network have poor credit histories, then you might receive a lower credit score than otherwise).

---

<sup>29</sup> There could also be flows in addition to those illustrated in this simplified diagram. For example, some merchants might interact with the issuing bank directly, and merchants and social networks might also exchange information.

**Figure 1**  
**Using Additional Information to Improve Credit Offers and Rewards Offerings**



43. *Rewards:* As also illustrated by Figure 1, the information collected by mobile payment networks and social networks could be used to improve payment-service rewards programs, such as airline mileage points offered for credit card use. Although card issuers collect considerable information about consumer transactions, to my knowledge no issuer today offers real-time, context-sensitive rewards. Consumer connectedness could change that. Sophisticated, real-time, context-sensitive payment-service rewards programs are enabled by the presence of consumer mobile access devices with form factors that allow the display of graphics. I will say more on this point when discussing the broader uses of consumer information in Section III below.

44. *Account management and customer service:* One drawback (at least from the consumer's perspective) of many if not most stored-value cards in use today is that they are not readily auditable by the user. In principle, a smart-phone-based stored value card could

also store a transaction history that was easily reviewable by the consumer. In addition, such a card could take advantage of consumer connectedness to allow remote recharging. More broadly, real-time communication with relevant financial institutions enables the provision of more sophisticated and up-to-date account management services, such as checking a credit account balance while in a store considering a purchase.

45. In summary, the analysis of this section suggests that the changes in pure payment services due to pervasive mobile connectivity and social networking will be evolutionary, not revolutionary. Pervasive mobile connectivity and social networking will facilitate payment service features that offer additional value to consumers and merchants. In many respects, however, mobile payments primarily will be an extension of various existing e-commerce payment options to a new set of Internet access devices. I also think that consumers will want the extension to be linked closely to existing systems. I suspect that many consumers do not want to have to use one payment instrument for online purchases made using a traditional personal computer and another payment instrument for online purchases made using a smart phone or tablet computer.<sup>30</sup>

---

<sup>30</sup> There may be limits to consumers' desire for one-stop shopping. For example, one interpretation of PayPal's success is that consumers want to have a limited account when transacting with merchants in whom consumers have less trust (this is my interpretation of PayPal's apparent appeal from hiding a consumer's credit card information from a merchant while potentially exposing the user's PayPal password. Of course, such preferences could be accomplished by a single payment mechanism that had different transaction and liability limits for different classes of merchants.

**III. IT'S ALL ABOUT THE BENJAMINS, AND THE BENJAMINS ARE ALL ABOUT THE INFORMATION**

46. If pervasive mobile connectivity and social networking are not going to revolutionize payment services, then why are so many people so excited about mobile payments? I believe some are excited because they are mistaken. But others are properly excited by the potential of mobile payment services (and social networks) to generate vast amounts of information about consumer behavior, which can then be sold for tens of billions of dollars annually. Indeed, it may turn out to be a profitable business model for a payment network to pay consumers and merchants to use its service so that the network can collect information that it then sells to advertisers and other businesses.

**A. I SAW WHAT YOU DID, I KNOW WHO YOU ARE.**

47. Connected individuals can be identified and tracked. Mobile payment transactions generate valuable information regarding current context and transaction histories.<sup>31</sup> As others have observed, context can include a wide variety of information, including “the location of the user, surrounding weather, user’s current yearn, social relations with nearby users, bandwidth of the user’s mobile device, screen size of the mobile device”.<sup>32</sup> Transaction histories may themselves include the contexts in which payment transactions were made and, potentially, even information about situations in which consumers shopped but did not complete purchases. In addition, consumers’ participation in social networks can allow the

---

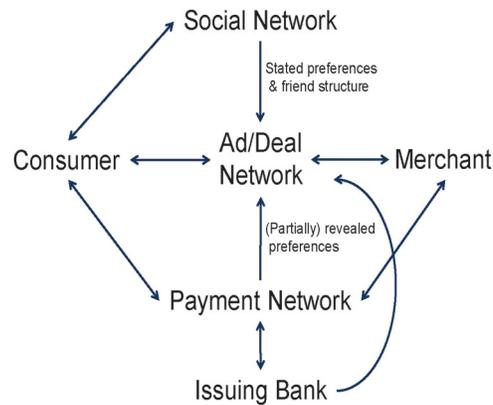
<sup>31</sup> As discussed below, consumers may also be connected through the facilities of the payment network itself.

<sup>32</sup> Janne Lukkari, Jani Korhonen, and Timo Ojala (2004) “SmartRestaurant: mobile payments in context-aware environment,” *ICEC '04 Proceedings of the 6th International Conference on Electronic Commerce*, Janssen, Sol, and Wagenaar (ed.s), 575-582 (hereinafter Lukkari *et al.* (2004)), at 576.

identification of an individual's revealed preferences (*e.g.*, what commercial postings he or she clicks on), stated preferences (*e.g.*, what approval or "like" buttons he or she clicks on and what recommendations he or she makes to others), demographic characteristics, sources of influence, and influencer value.

48. Figure 2 provides an illustrative schematic of some of the most important information flows

**Figure 2**  
**The Art of the Deal Network**



It is important to note that this diagram identifies different conceptually distinct functional roles. In practice, a single enterprise might serve as the social network, ad/deal network, and payment network.

49. The information collected through mobile payments and social-network based payments could be valuable in multiple uses. As discussed above, some uses are directly rated to payment services, particularly the offering of consumer credit. But the far greater

value will come from uses outside of the traditional payments sector. Once connected individuals have been identified and tracked, and their behavior analyzed, they can be sent personalized, context-specific communications from merchants as part of broader relationship-management strategies.

50. The context on which the communications are customized can include elements of the consumer's current status (*e.g.*, whether he or she is near a particular coffee retailer, the time of day, and evidence whether he or she has recently purchased coffee) and also certain aspects of the merchant's current status (*e.g.*, whether the restaurant is crowded or empty, or whether the retailer has an excess stock of certain products). In terms of relationship management, sales histories can play a large role and can allow a merchant to reward its "loyal" customers with special deals.<sup>33</sup> A merchant could even offer social loyalty programs, whereby the deals offered to a set of consumers are related to the consumers' collective actions.<sup>34</sup>

51. Consumers' current contexts and transaction histories could, in theory, be used to: (a) support programs of personalized pricing and customized offers or deals; (b) improve the targeting of advertising (including direct mail, robo-calls, and various forms of online ads); and (c) improve the quality of Internet search. For example, Facebook allows advertisers to target their audience with reference to users' location, language, education, work, age, sex,

---

<sup>33</sup> I place the word loyal within quotation marks because one might argue that truly loyal customers do not require special deals to be induced to patronize the merchant.

<sup>34</sup> By way of comparison, Groupon currently facilitates offers that are sensitive only to the merchant's context (and not in real time) and that are very crude in terms of relationship management. Although in at least some cases intended to serve as introductory offers that begin longer-term relationships, the big discounts associated with Groupon deals may encourage an adversarial attitude of consumers toward merchants. Groupon has what some observers label a "social" element, but it is among strangers and is not—in my view—properly viewed as a loyalty program.

birthday, relationship status, likes and interests, whether they are fans of the advertiser's Facebook page, and whether they are friends of fans of the advertiser's Facebook page.<sup>35</sup> Moreover, if it could be aggregated, the information from social networks combined with that from payment networks could create powerful measures of a consumer's influence on other consumers, and many businesses are willing to pay to identify major influencers.

**B. SEARCHING NEAR OR FAR FOR A VALUE PROPOSITION**

52. As were several earlier years, 2012 is supposed to be the year general-purpose payment products based on near-field communication (NFC) take off. I am doubtful.<sup>36</sup> This doubtfulness springs from the fact that other wireless technologies, such as WiFi and traditional cellular networks, offer a broader range of possibilities and greater potential for value creation.

53. NFC can provide some incremental benefits in the form of added convenience and functionality at check out. For example, some consumers would very likely prefer to waive their phones in the air rather than swipe their payment cards in a traditional reader, and NFC could support additional promotional activity at check out, similar to existing instant coupons generated at check out. Hence, NFC may make sense for the established payment networks, such as MasterCard and Visa, because it provides their users one more option and may be a particularly useful alternative for merchants with high volumes of low-value transactions.

---

<sup>35</sup> See <http://www.facebook.com/business/ads>, site visited April 20, 2012.

<sup>36</sup> I believe that NFC is more likely ultimately to be remembered as "never fulfilled claims." Those readers with telecommunications backgrounds will recognize this prediction as a tribute to the person who first observed that ISDN stood for "it still does nothing," rather than "integrated services digital network."

54. The really exciting possibilities, however, come from communication between the consumer and merchant *before* the consumer gets to the checkout line.<sup>37</sup> The widespread adoption of smart phones and other mobile devices with increasing capabilities is making possible new services and products that will revolutionize the interactions between consumers and merchants.

55. The potential for mobile communications between a merchant and a consumer not next to the POS transaction-capture device (what might be termed “far field communication”) has long been recognized. One example is a service known as SmartRestaurant, which was tested over eight years ago. This service allowed a customer to use his or her mobile access device to view a menu, place an order, pay for the order, and set a pick-up time.<sup>38</sup> In comparison with in-establishment ordering, the consumer benefited from being able to order and pay from a convenient location and then go through a much quicker pick-up process. The merchant benefited from having additional time to plan and adjust food preparation.<sup>39</sup>

56. One aspect of the service that was critical to enabling these consumer and merchant benefits was that the service made use of communication *before* the consumer reached the checkout counter. Indeed, the consumer and merchant communicated with one another before the consumer was even at the merchant’s site. Of course, people have been faxing lunch orders for many years. And now, people can submit orders using a fixed-line Internet or mobile connection. In that respect, these are evolutionary changes.

---

<sup>37</sup> Like a dog taught to walk on two legs, NFC could do other things. NFC swiping stations could be set up in the store aisles or showrooms so that consumers could seek information on the products and available deals.

<sup>38</sup> Lukkari *et al.* (2004) at 576.

<sup>39</sup> *Id.*

57. With the rise of location-aware devices, the possibilities for communication between merchants and nearby consumers become far greater and the nature of the communication can fundamentally change. For instance, several vendors are making use of geofencing technologies, whereby a potential customer is sent promotional messages if he or she comes in proximity to a designated retail outlet.<sup>40</sup> In October 2010, for example, Starbucks teamed with the wireless network operator O2 to offer a geofencing program promoting Starbucks' Via instant coffee. When a participating consumer was sufficiently near a Starbucks store or a grocery store that sold Via, a discount coupon was issued via SMS.<sup>41</sup> More generally, the message sent to a consumer as part of a geofencing program can contain: special pricing; information about the retail location's address, contact information, and operating hours; and information about the availability of specific products.<sup>42</sup>

58. The Pay with Square service described above also relies on geofencing, in this case 100-meter geo-fences based on WiFi.<sup>43</sup> The geofencing allows the consumer to "set up

---

<sup>40</sup> See, for example, Chantal Tode, "Will wide-scale adoption of geofencing happen this year?" *Mobile Commerce Daily*, April 16, 2012, available at <http://www.mobilecommercedaily.com/2012/04/16/geofencing-strategies-on-the-rise-but-challenges-remain>, site visited April 20, 2012.

<sup>41</sup> Placecast, "O2 Case Study," available at [http://placecast.net/research/case\\_study\\_o2.pdf](http://placecast.net/research/case_study_o2.pdf), site visited April 20, 2012, at 01.

<sup>42</sup> For a description of one such service, see <http://placecast.net/shopalerts/operators.html>, site visited April 20, 2012.

<sup>43</sup> <https://help.squareup.com/customer/portal/articles/223248-new-how-do-i-set-up-auto-open-in-card-case->, site visited April 20, 2012.

Square to automatically open your tab when you walk in the door” of a merchant.<sup>44</sup>

According to Square, there is no need for the consumer to touch his or her phone or wallet.<sup>45</sup>

59. One could easily imagine other microfencing applications along these lines. For instance, a consumer might visit a bricks-and-mortar retailer, pick up the desired items, and then simply walk out of the store. RFID tags on the items, coupled with identification of the consumer’s mobile access device, could be used to generate an automatic charge to the relevant payment account. Clearly many other opportunities for innovative new services exist.

#### C. WHO WILL CONTROL CONSUMER INFORMATION?

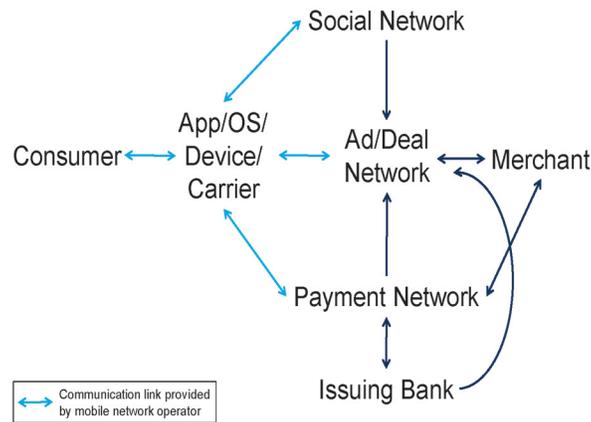
60. If information is where all the money will be, then intense battles to own and control access to that information can be expected. Figure 3 illustrates the information channels that may be wireless, and it provides a finer breakdown than does Figure 2. As Figure 3 illustrates, potentially one or more of the following groups might control important pieces of consumer information: wireless carriers, mobile access device manufacturers, mobile OS developers, app developers, consumer banks, and payment networks. Consequently, there may be struggles for control that cut across the telecommunications, financial services, and web services sectors. There may also be struggles within each sector. For example, app developers, mobile access device OEMS, mobile OS providers, and wireless carriers all may lay claim to consumer information related to mobile payments.

---

<sup>44</sup> <https://squareup.com/pay-with-square>, site visited April 20, 2012.

<sup>45</sup> *Id.*

**Figure 3**  
**Who will Control Consumer Information?**



61. Within the financial sector, MasterCard and Visa may have disagreements with card-issuing banks with respect to who has the rights to use transaction information. At least for now, both Visa and its issuing banks appear to be able to use the information:<sup>46</sup>

Gap and Visa began a pilot of [a] real-time text message system in November [2010]. Customers enrolled via a secure website and were sent Gap offers when they used their Visa cards to complete transactions that met certain criteria -- for example, they may have had to buy something at a store in a specified ZIP code, or shop during a certain time period. Once the offers appeared on their phones, the customers took advantage of them by showing

<sup>46</sup> Matt Hamblen, "Visa, Gap use text messages to mobile phones for promotions," *Computerworld*, April 21, 2011, available at [http://www.computerworld.com/s/article/9216060/Visa\\_Gap\\_use\\_text\\_messages\\_to\\_mobile\\_phones\\_for\\_promotions](http://www.computerworld.com/s/article/9216060/Visa_Gap_use_text_messages_to_mobile_phones_for_promotions), site visited April 28, 2012. See also, Sarah Perez, "Visa Launches Real-Time, Location-Based Discounts for Gap Customers," *ReadWriteWeb*, April 21, 2011, available at [http://www.readriteweb.com/archives/Visa\\_launches\\_real\\_time\\_location\\_based\\_discounts\\_for\\_gap\\_customers.php](http://www.readriteweb.com/archives/Visa_launches_real_time_location_based_discounts_for_gap_customers.php), site visited April 28, 2012.

the text messages to Gap sales clerks.

This pilot is notable because it is my understanding that this relationship between Visa, Gap, and consumers was not mediated by either a card-issuing bank or a merchant-acquiring one.<sup>47</sup>

62. One could even imagine consumers controlling their own information. For example, a consumer might have a low-cost app that allowed him or her to control who had access to his or her personal information, with the possibility of demanding compensation for the right to use this information. Here, pervasive social network poses some interesting difficulties. Would your friends be allowed to sell or give away what they know about you even if you refused to provide the information yourself? In any event, I believe that it is implausible that American consumers will go to the trouble of managing their information to this degree unless it is made very easy to do so.

63. “Ownership” of “the” customer relationship is often seen as critical point of strategic control in economic ecosystems and might be seen as a way to control access to consumer information. However, there may be multiple customer relationships that come into play simultaneously in the area of mobile payments. A consumer may perceive him- or herself as having one relationship with a mobile carrier, another with a mobile access device OEM, and a third relationship with a financial institution. Moreover, depending on public policy and private contracts, a firm might have access to a consumer’s information even if that consumer does not perceive him- or herself as having a meaningful commercial relationship.

---

<sup>47</sup> It is also notable in that it uses Visa’s network to provide the location service and uses wireless networks solely for SMS messages, so that smart phones are not required and wireless carriers play a very limited role in providing the service.

**D. REGULATION, REGULATION, REGULATION**

64. Legal and regulatory decisions regarding privacy and antitrust will very likely be critical determinants of who controls consumer information. For instance, as discussed below, the only way that I can see mobile network operators' being able to capture a large part of the value created by mobile payments services is if they could successfully limit the set of access devices operating on their mobile networks and the applications that run on those devices (*i.e.*, if wireless carriers could control who offered mobile payment services over their networks). Hence, telecommunications-specific and economy-wide antitrust regulation will play important roles in shaping industry evolution.

65. The public-policy treatment of privacy and information ownership are likely to play very significant roles in the *creation*, as well as capture, of value from new services based on payment products enable by pervasive connectedness.<sup>48</sup> For example, a study of European privacy regulation found that it substantially reduced the effectiveness of targeted advertising.<sup>49</sup>

66. The convergence of three economic sectors is also going to involve the convergence (or collision) of three or more regulatory regimes. For example, telecommunications carriers and financial institutions are subject to distinct, sector-specific privacy regulation and antitrust

---

<sup>48</sup> To the extent that privacy regulation distinguishes uses of information within an enterprise from uses that cross enterprise boundaries, regulation could affect enterprise's choices of their boundaries. For instance, public policies that are more lenient toward within-enterprise transactions are likely to promote greater enterprise scope. Similar issues can arise with respect to antitrust policy when two divisions of a given enterprise are permitted to engage in practices (*e.g.*, exclusive contracting) that might be found to be antitrust violations if practiced by two separate enterprises.

<sup>49</sup> Avi Goldfarb and Catherine Tucker (2010) "Privacy Regulation and Online Advertising," available at <http://ssrn.com/abstract=1600259>, site visited May 1, 2012.

enforcement regimes. And web services companies have been drawing attention from the Federal Trade Commission. Thus, the use of information about a consumer's mobile payment transactions could be subject to oversight from three or more different agencies.

67. In addition to creating the potential for regulatory conflict, the presence of multiple regimes may lead to consumer confusion. Consider, for example, direct carrier billing, which allows a consumer to make a purchase (e.g., buy a smartphone app) and have the charges posted on his or her wireless service billing account. According to ConsumerReports.org,<sup>50</sup>

Federal law currently offers protection to consumers in the event that their credit card or debit card is lost, stolen or misused. ... If mobile payment transactions are linked to credit cards or debit cards, then consumers are entitled to the same guaranteed federal protections that apply when a credit card or debit card is used directly in a transaction.

Mobile charges linked to other forms of payment don't enjoy any of these legal protections. If the mobile payment charge appears on the customer's cell phone bill, the product might escape consumer protections entirely unless the contract provides them.

Given how few consumers read contracts, it would seem unlikely that consumers know the extent of their protections with direct carrier billing.

68. Although industry members often are adverse to regulation, it should be noted that certain forms of regulation may make an important contribution to the success of mobile payments. In their recent study of consumers, Andreev *et al.* (2011, p. 123) found

conclusive evidence of the association between trust and consumer's willingness to make an m-payment using a smart phone. By exploring trust in detail, our analysis illustrates that consumer's [sic] perceptions of legal frameworks and the regulation of these frameworks are integral parts of trust.

---

<sup>50</sup> ConsumerReports.org, "T-Mobile's "Direct Carrier Billing" Program Could Leave Consumers Vulnerable," August 8, 2011, *available at* <http://pressroom.consumerreports.org/pressroom/2011/08/t-mobiles-direct-carrier-billing-program-could-leave-consumers-vulnerable.html>, site visited January 25, 2012.

In addition to refusing to adopt mobile payments, consumers may engage in self-help to deal with privacy concerns by providing only limited or false information about themselves.<sup>51</sup> From the industry's perspective, regulation may be preferable to any of these outcomes.

#### IV. GETTING FROM HERE TO THERE

69. It sometimes seems that each year begins with the prediction that it will be the year mobile payment services take off (with or without NFC) and ends with the prediction that the *next* year will be the one in which the take-off will occur. If mobile payments services are so great, what is holding them back? One possibility is that, even when one accounts for the value of the information generated by mobile payment services, the benefits are always going to be less than the costs. I think the more likely answer is that, although the benefits outweigh the costs in the long term, there are difficult start-up issues that must be overcome to realize the potential benefits.<sup>52</sup>

70. On the merchant side, Mallat and Tuunainen (2008, p. 24) found that “the barriers to adoption include complexity of the systems, unfavorable revenue sharing models, lack of critical mass, and lack of standardization.” On the consumer side, Mallat (2007, § 5.6) found that the lack of widespread adoption by merchants was a deterrent to adoption by consumers.

---

<sup>51</sup> Peter O'Connor (2005) “Comparative Analysis of International Approaches to the Protection of Online Privacy,” in S. Krishnamurthy, ed., *Contemporary Research in E-Marketing*, Vol. 2. Hershey, PA: Idea Group Publishing, as summarized by Evelyn Beatrix Cleff, (2007) “Implementing the Legal Criteria of Meaningful Consent in the Concept of Mobile Advertising,” *Computer Law and Security Report*, 23(3): 262–269, at 265.

<sup>52</sup> I don't subscribe to the conspiracy theories of the sort put forth by several of the people interviewed in a recent Pew Research Center survey. (Aaron Smith, Janna Anderson, Lee Rainie, “The Future of Money: Smartphone Swiping in the Mobile Age,” Pew Research Center, April 17, 2012, available at <http://www.pewinternet.org/Reports/2012/Future-of-Money.aspx?src=prc-headline>, site visited April 28, 2012 (hereinafter, Smith et al. (2012)) at 5, 16, and 17.)

And, as discussed in Section II.A.2 above, Dewan and Chen (2005), Viehland and Leong (2007), and Andreev *et al.* (2011), among others, found that consumer concerns about security and privacy were significant obstacles.

#### A. CONSUMER TRUST

71. Consumers' security and privacy concerns have been identified as barriers to the adoption of mobile payments. However, as noted above, American consumers have a history of saying that they care more deeply about privacy and security than their actual behavior suggests. I believe that people will continue to express concern about security and privacy but in the long run they will act as if they are unconcerned. In the short run, however, the lack of trust in mobile payment systems can be an impediment to adoption.

72. One solution is to have mobile payments offered by established firms that have already have good reputations and are trusted by consumers. In their survey of consumers, Andreev *et al.* (2011, p. 117) found "that respondents considered using a secure and trusted third-party payment company as the preferred method of making an m-payment for products/services." Similarly, Mallat (2007, p. 424) concluded that focus group participants were "more willing to conduct payments with trustworthy transaction parties and regarded established banks, credit card companies, and telecom operators as reliable mobile payment service providers. Banks were slightly preferred to other providers."

### B. NETWORK EFFECTS AND THE CHICKEN-AND-EGG PROBLEM

73. Network effects arise when, the greater the number of users on a system, the more valuable the system is to an individual user.<sup>53</sup> Network effects are prevalent in payment services. An increase in the number of consumers making use of a given payment service will—if the costs are not too high relative to the benefits—make acceptance of that payment service more attractive to merchants. And, all else equal, a consumer will more highly value a payment service the more extensive is the merchant acceptance network for that payment instrument. These positive relationships between the number of one type of payment-service user and the other are examples of what economists refer to as *cross-platform network effects* because they involve two different groups of platform users each of which values the presence of members of the other group.<sup>54</sup> Although the most obvious network effects are those associated with merchants and consumers, there are also cross-platform network effects in the supply of complementary products, such as smart phones and merchant POS devices that can communicate with one another.<sup>55</sup>

---

<sup>53</sup> For a survey of the economics of network effects, see Michael L. Katz and Carl Shapiro (1994) “Systems Competition and Network Effects,” *Journal of Economic Perspectives*, 8 (Spring): 93-115 (hereinafter, Katz and Shapiro (1994)).

<sup>54</sup> For survey of cross-platform network effects, also known as two-sided markets, see Roberto Roson (2005) “Two-Sided Markets: A Tentative Survey,” *Review of Network Economics*, 4(2): 142-160.

<sup>55</sup> In addition, positive-feedback effects may arise with respect to the provision of targeted-marketing services to merchants. Specifically, the larger a payment-service’s merchant-acceptance network, the greater the depth of information that service will be able to collect about its consumer users because the payment service will likely capture a greater percentage of any given consumer’s transactions. Hence, the greater the number of merchants using a payment service, the higher the value of the targeted marketing services that platform can offer to merchants.

74. An important implication of network effects is that a payment network can suffer from a “chicken-and-egg problem.” In short, a chicken-and-egg problem arises when no one wants to belong to a network unless lots of other parties belong to the network first. Specifically, a merchant will not want to bear the expenses of changing its checkout process to accommodate a new payment service if there are few consumers who would potentially use that service. Similarly, a consumer will not want to sign up for the payment service if there are few merchants who accept it. Of course, if everyone waits for lots of other parties to join the service, then the service will never get off of the ground.

75. There are several potential solutions to the chicken-and-egg problem. One is to begin with smaller groups that have strong cross-platform network effects among themselves. One of the most successful examples of mobile payments to date is the mobile app version of Starbucks pre-paid store cards. The CEO of the developer of the Starbucks application attributed this success to “factors like Starbucks’ complete control over the point of sale, the use of a closed-loop system, and smartphone-toting customers who are loyal and often make daily visits to the brand.”<sup>56</sup> In addition, approximately 20-percent of Starbucks customers’ in-store purchases were made using Starbucks’ loyalty card before the app was launched.<sup>57</sup>

76. Another approach is to adopt pricing strategies that make joining a service attractive even if, at present, it offers relatively few benefits. One such strategy is penetration pricing, whereby prices are initially set at low (possibly below-cost) levels in order to attract users to

---

<sup>56</sup> “POS Gets Smart,” *QSR*, June 24, 2011, available at <http://www.qsrmagazine.com/news/pos-gets-smart>, site visited March 11, 2012. [The quotation in the text is of the cited article’s paraphrase of what the executive said.]

<sup>57</sup> *Id.*

the service. As the service becomes established, prices can be increased. A variant of across-the-board penetration pricing is to offer special deals solely to key early adopters. Specific parties may be particularly important early adopters for at least three reasons. Early adopters can: create valuable positive network effects (*e.g.*, a popular merchant will attract buyers to the payment service); help the network achieve an efficient scale of operation; and, in some cases, add credibility.

77. A payment service could also offer users subsidies to cover fixed costs of participation. For example, a merchant typically has to incur fixed costs (*e.g.*, the costs of modifying online shopping cart software) to participate in a payment service. If the merchant later determines that it is undesirable to participate in the service, then these costs will be lost. Hence, these costs represent a risk of participating and create an incentive to wait until other parties have joined a new service and shown it to be viable. Development subsidies are one way to reduce the risks of membership and thus lessen the chicken-and-egg problem. Offering free applications to consumers has a similar effect.

78. In market with strong network effects, the degree to which different services are interoperable, or compatible, can also affect adoption decisions, as well as industry performance generally. Compatibility can reduce costs by allowing different service providers to share some elements of infrastructure (*e.g.*, POS transaction-capture devices). Users may also be more likely to adopt new payment services because there is less threat of lock-in or stranding when a given piece of user equipment (*e.g.*, a smart phone) can operate with multiple services. Hence, the chicken-and-egg problem is less severe.

79. But compatibility can also reduce or eliminate network size as a source of competitive advantage. Consequently, firms that have large installed bases—or firms that users generally *expect* to be particularly successful under incompatibility—may oppose compatibility.<sup>58</sup> Moreover, particular standards may favor some service providers over others. Hence, it is not a foregone conclusion that widespread standards will be adopted and compatibility achieved simply because network effects are present.

80. That said, I believe there will be standardization of merchants' POS transaction-capture devices. Merchants will likely exhibit very strong preferences for compatible POS transaction-capture devices, as we have today with different credit, charge, and debit card readers. Most merchants have limited space at checkout, and what they space they do have could better be used to display products rather than house multiple payment terminals.<sup>59</sup> Because the demand for compatibility among POS transaction-capture devices will be so strong, I expect that the most widely adopted devices will work with multiple payment services and will drive consumer mobile access devices to have similarly standardized interfaces. Although these devices will be standardized, there will still be significant opportunities for the payment services making use of these devices to differentiate themselves from one another.<sup>60</sup>

---

<sup>58</sup> See, for example, Katz and Shapiro (1994).

<sup>59</sup> Note that this issue need not arise in this exact form for certain payment services based on WiFi and cellular networks. However, these technologies, too, will require at least some equipment located on the merchant's premises.

<sup>60</sup> Economic theory suggests that widespread compatibility that allows product differentiation would very likely maximize the joint profits of competing payment-service providers. Consumers and merchants might be reluctant to adopt a monopoly service, thus exacerbating the chicken-and-egg problem, while a lack of differentiation could lead to intense payment-

81. In addition to issues regarding standardization across competing mobile payment services, there are also issues regarding standardization across mobile payment services and existing payment services. Compatibility with existing services can reduce the chicken-and-egg problem for new services. These considerations arise with respect to NFC. Here, the desires of at least some parties to maintain compatibility are evident.<sup>61</sup>

Visa has played a leadership role in establishing global standards for mobile payments, making sure that they are aligned with existing technology and security standards for chip payment cards and can easily be integrated into the existing payments ecosystem. For example: Visa payWave on mobile devices is compatible with existing contactless (NFC) payment terminals already installed at retail outlets worldwide, enabling Visa account holders to simply wave their enabled phone in front of a payment terminal in order to pay.

82. Compatibility with existing systems is also valuable because, even if most consumers rely on their mobile phones to serve as smart cards, merchants will still have to deal with non-phone-enabled consumers for a significant period of time. Thus, compatibility will allow merchants avoid the costs of having to operate two systems simultaneously.

83. The chicken-and-egg problem faced by payment services is not limited to consumers and merchants. These effects also apply to financial institutions and other potential complementors, such as mobile access device OEMs which must choose whether to install special features such as NFC chips on their devices. One solution to the complementor

---

service competition that eroded profits. From a social welfare perspective, a structure that allows service providers to differentiate themselves can spur innovation and long-run competition.

<sup>61</sup> Rebecca Robinson, "Smart Phones for Use as Visa Mobile Payment Devices," *CardGuide*, 21 February 2012, available at <http://www.card-guide-international.com/201202211911/Visa-Certifies-Smartphones-for-Use-as-Visa-Mobile-Payment-Devices.html>, site visited March 11, 2012.

version of the chicken-and-egg problem is for the payment service either to subsidize the production of the complements or to purchase them on behalf of users.

84. Several years ago, Wells Fargo tested a service that allowed users to make payments using a phone rather than a bankcard. Wells Fargo chose not to offer the service to its customers, in part because there was only one handset that could be used to offer the service.<sup>62</sup> Even today, most smart phones do not have built-in capabilities to communicate with merchant POS devices. Recently, however, Wells and other potential payment providers have experimented with microSD cards that can add these capabilities to existing phones,<sup>63</sup> and DeviceFidelity and Spring Card Systems announced a microSD card that can be inserted into an Android phone and used to make payments over MasterCard's PayPass NFC system.<sup>64</sup> These developments highlight the need for complementary investments at various points in the value net. They also illustrate how some parties may be able to internalize complements effects by offering the complementary products to their customers rather than waiting for independent suppliers to offer them directly to users.

---

<sup>62</sup> Rachael King, "Wells Fargo tests smart-phone mobile payments," *SFGate*, January 5, 2011, available at <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/01/04/BUBT1H3TO3.DTL>, site visited March 11, 2012.

<sup>63</sup> *Id.* See also Andrew Johnson, *In Mobile Payments, Lack of Interoperability Threatens Adoption*, *American Banker*, Dec. 9, 2010, available at [http://www.americanbanker.com/issues/175\\_235/lack-of-interoperability-1029690-1.html](http://www.americanbanker.com/issues/175_235/lack-of-interoperability-1029690-1.html), site visited March 11, 2012.

<sup>64</sup> Mat Smith, "Moneto NFC microSD to bring contactless features to any Android phone," *engadget*, posted January 11, 2012, available at <http://www.engadget.com/2012/01/11/moneto-nfc-microsd-contactless-payment-Android-iPhone/>, site visited April 28, 2012.

## V. WHO WILL DO WHAT?

85. Having discussed many of the forces that will shape competition, I next examine what roles will be played by the various payments industry participants, including banks, wireless telecommunications service providers, financial institutions, traditional card payment networks, and web services companies.

### A. DON'T GET CARRIED AWAY WITH CARRIERS

86. Wireless carriers will unquestionably provide important communication links that will enable both mobile payment services and mobile advertising-and-deal services. Figure 3 above illustrates the fact that wireless carriers will provide communication links between consumers and payment networks, deal-and-advertising networks, social networks, and—directly or indirectly—merchants. Despite the importance of these links, it does not follow that wireless carriers will be successful in capturing the value created by these services.

87. Indeed, there is a wide variety of opinions regarding whether wireless network operators are like to succeed in capturing value, ranging from extreme optimism<sup>65</sup>

There is a game-changing opportunity here for the operators to effectively displace credit cards and banks.

to strong pessimism<sup>66</sup>

Operators will continue to attempt to insinuate themselves into the process at a premium rather than simply accepting their long-term fate of being minimum-margin bit pipes for the masses.

---

<sup>65</sup> Dan Hays of PRM as quoted by Leila Abboud, “Telcos battle tech, bank titans for mobile payments,” *The Globe and Mail*, February 14, 2011, available at <http://m.theglobeandmail.com/news/technology/mobile-technology/telcos-battle-tech-bank-titans-for-mobile-payments/article1905892/?service=mobile>, site visited April 28, 2012.

<sup>66</sup> Rob Scott of Nokia as quoted by Smith *et al.* (2012) at 14.

Other commentators fall in the middle, seeing mobile network operators as playing critical roles but doing so by partnering with financial institutions rather than displacing them.<sup>67</sup>

88. In my opinion, the pessimistic view is very likely the correct one: telecommunications providers will neither significantly shape the evolution of general purpose payments in the United States nor will they capture significant value. Instead, they will provide essential but undifferentiated infrastructure.<sup>68</sup> The term “undifferentiated” is critical here. It will prevent almost all access device OEMs and telecommunications carriers from having powerful positions within the mobile payments value net (the one exception may be Apple). There is little or no need to have wireless network operators involved in planning payment services, and there is relatively little benefit to other parties from forming alliances with mobile network operators except in their roles as distributors of mobile access devices.<sup>69</sup> In addition, wireless carriers and access device manufacturers generally lack strong business relationships with merchants.

---

<sup>67</sup> See, for example, Jan Ondrus and Kalle Lyytinen (2011) “Mobile Payments Market: Towards Another Clash of the Titans?” *Proceedings of the 10th International Conference on Mobile Business*, Como, Italy.

<sup>68</sup> Telecommunications firms may play much more significant roles in developing economies (*Id.*, §I):

Some local success stories have been observed in developing countries... However, these systems have been well adapted for the financial markets of the developing world (e.g., high penetration of mobile phones, low bank service penetration, lack of alternative solutions, clear economic value propositions for the users.). Those contexts are highly specific and far from the ones encountered in the developed world.

<sup>69</sup> That said, several such parties apparently disagree with my assessment and have formed alliances with wireless carriers.

89. Mobile network operators do not want to be commoditized, “dumb pipes.” But to avoid this fate, network operators have to provide something that cannot better be provided at the edge (either for technological reasons or because network operators have locked out rivals).

90. Experience with fixed-line access to the Internet does not bode well for mobile network operators and access device OEMs. Personal computer manufacturers, operating system developers, and Internet service providers play no role in online payments today beyond providing generic infrastructure over which online payment applications run. And there is no reason to expect that situation to change. I don’t know of anyone who expects fixed-line broadband Internet service providers to dominate online payments. Why should one expect mobile broadband providers be any different?

91. There are a few possible reasons. For one, mobile broadband service providers in the United States have been able to keep much greater control over how their services are used than have fixed-line providers. For example, wireless carriers can limit the set of devices used to access their networks and have some degree of control over the applications that run on those devices. But blocking competing payments services would be very difficult.

92. It would be relatively easy to work around bottlenecks in mobile access devices that took the form of proprietary chips or capabilities. Even if there were proprietary NFC chips installed in smart phones by OEMs or carriers, there are add-on chips and software solutions that can be utilized instead. And, of course, WiFi- and cellular-based systems need not rely on NFC at all. In order to keep competing payment services from reaching its customers, a mobile network operator would have to rely on more actions specifically designed and

targeted to block those applications. I question whether excluding mobile payment applications in that way is a feasible long-term strategy either commercially or politically.

93. The two earlier discussions the Starbucks app and bank's use of microSD cards to run an over-the-top payment application illustrate some of the difficulties that mobile network operators and access device OEMs face. There is no need for wireless carriers, wireless OS providers, or mobile access device manufacturers to provide any features or functions specifically tailored to the Starbucks app. Although banks consider microSD cards to be a transition technology,<sup>70</sup> these cards demonstrate the existence of a simple work-around of any device manufacturer and carrier that attempted to go a different route (as long as the devices had non-proprietary expansion slots; once again, Apple may be different than the rest of the industry).

94. The other way to avoid becoming "dumb pipes" is for mobile networks to provide something that is cannot—or at least is not today—better provided at the edge. For example, network operators may be able to provide some information that, although edge devices could provide, many do not. Locaid Technologies, Inc., and Placecast offer geofencing services that use mobile network information to determine a subscriber's location.<sup>71</sup> Consequently, these services are available to consumers who do not have GPS-enabled phones. Although this approach may be valuable in the short run, it seems likely that, in the long run, a very high

---

<sup>70</sup> Rachael King, "Wells Fargo tests smart-phone mobile payments," *SFGate*, January 5, 2011, available at <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/01/04/BUBT1H3TO3.DTL>, site visited March 11, 2012.

<sup>71</sup> <http://www.loc-aid.com/about-us>, site visited April 20, 2012; Ryan Kim, "O2 Turns on Geofencing for Starbucks, L'Oreal in UK," *GigaOm*, October 14, 2010, available at <http://gigaom.com/2010/10/14/o2-turns-on-geo-fencing-for-starbucks-loreal-in-uk/>, site visited April 20, 2012.

percentage of mobile access devices will be location aware, whether by using GPS, triangulation based on WiFi networks, or some other means. Moreover, in the long run, those devices that are not location-aware may be feature phones that lack the ability to provide rich graphics and, hence, will rely on SMS messages that are much less powerful marketing tools than those that can be provided to smart phone and mobile tablet users. I am unaware of any other services or features relevant to payment systems that can be offered by the core of mobile networks but not edge devices.

95. There may be certain niches (albeit multi-billion-dollar niches) in which mobile network operators play deeper roles. For example, carrier-based billing is convenient for purchasing apps, ringtones, and similar digital goods for use on mobile devices. And SMS-based and carrier-based-billing solutions might have a place for low-value, spontaneous transactions (*e.g.*, to pay for online voting related to a television broadcast). For mainstream mobile payments, however, mobile network operators' roles are likely to be limited.

96. Similar considerations arise with respect to mobile operating system providers and access device OEMs. Although, in at least some instances, these parties may be more differentiated along other dimensions, they still will serve as relatively undifferentiated infrastructure for over-the-top payment services unless they are able actively to lock out such competitors. With the possible exception of Apple, such a strategy seems infeasible for access device manufacturers given the high degree of competition they face. And such a strategy seems unlikely for Microsoft and RIM given their weak market positions, and Android given its open strategy.

**B. GIVE BANKS CREDIT**

97. My analysis suggests that the roles of financial institutions play in payment systems will not change very much as the result of increasing consumer connectedness. There are two dimensions to this prediction: (a) banks will not branch out to play significant new roles; and (b) other types of institutions will not displace banks as sources of credit and stores of wealth.

98. My basis for prediction (a) is two-fold. First, with the exception of the bank controlled by American Express, few if any banks have a broad enough customer bases to attract merchants to a proprietary network based on a single bank's consumer customers. Second, I expect banks to be able successfully and profitably to extend their traditional roles of providing credit and serving as stores of wealth to mobile payments by partnering with other parties that are better positioned to develop merchant networks and the other aspects of new payment systems.

99. Given the existence of various regulatory constraints, prediction (b) might almost be true by definition: enterprises taking over banks' roles will have to become banks themselves. The more interesting version of this prediction is that mobile payments will not allow significant entry of new firms as suppliers of credit, at least in the short run.

100. This prediction is based on the fact that issuing credit is hard work. Just ask AT&T or American Express. AT&T believed that the core competence needed to issue credit cards was the ability to process large numbers of transactions efficiently and reliably. Given its experience in large-scale, highly complex telephone billing, AT&T thought it had this competence. AT&T entered the card-issuing business and amassed a large portfolio. However, the credit card industry evolved so that a critical—or, perhaps, the critical—skill is

the ability to process information to predict what card offers will appeal to consumers and which consumers will be profitable. AT&T lacked this skill and exited the industry by selling its credit card portfolio to Citibank.

101. American Express also serves as an instructive example of the difficulties of issuing credit cards without experience or an existing customer base. American Express initially had significant difficulties when it first issued a credit (as opposed to charge card). When it began offering its Optima credit card in 1987, American Express dramatically misjudged the market and the risks that it faced.<sup>72</sup> Consequently, American Express ended up suffering loan losses of hundreds of millions of dollars per year between 1988 and 1994, despite being an experienced charge card issuer and having account histories for millions of charge card holders.<sup>73</sup> Since becoming an experienced credit card issuer, American Express has become more successful.

102. Banks have another competitive advantage in addition to their experience issuing credit. As discussed in Section IV.B above, some researchers have found that consumers place greater trust in established payment companies and banks. This factor speaks well to a continuing, central role for banks and the existing bankcard payment networks.

103. Lastly, it should be observed that there is a further connection between parts (a) and (b) of this prediction: because banks have an important and profitable role to play as a

---

<sup>72</sup> According to Bernstein Research, once American Express launched the Optima card, “Disaster followed. The list of what went wrong is almost unbearably long. The credit assumptions were flawed to begin with,…” (“The Future of the Credit Card Industry: Part II—Company Outlook,” Bernstein Research, January 1996, at 30.)

<sup>73</sup> *Id.*, Exhibit 18 and accompanying text.

complementary piece, they do not have large incentives to try to create proprietary systems of their own.

**C. WITHER INCUMBENT PAYMENT CARD NETWORKS?**

104. Many people see the developments discussed in this paper as very significant threats to incumbent payment card networks. It is important to recognize that many of these developments also represent opportunities for incumbent networks. These developments extend the reach and increase the utility of the services offered by these networks. Incumbent payment card networks may be able to take advantage of these opportunities directly. These networks have several competitive advantages including: reputations with consumers for trustworthiness; large merchant acceptance networks; and lots of data, including data generated by non-mobile transactions. For incumbent payment card networks, the biggest question is whether they have the organizational capabilities to innovate successfully to build on their current strengths.

105. Even if incumbent networks do not take advantage of the opportunities created by pervasive consumer connectedness directly, many of the services offered by companies such as PayPal and Square are built on top of the services of incumbent card networks. That said, there is a risk that some of these complementary service providers may evolve into competitors.

**D. WEB-SERVICES COMPANIES**

106. The rise of Internet payments has brought web-services companies such as eBay, Google, and Facebook into the payment arena. Many of these companies are essentially information collection-and-processing companies, with valuable competitive assets that include: massive

amounts of consumer data; experience efficiently collecting, storing, and processing that data at scale; high degrees of skill at processing the data to model consumer behavior (*e.g.*, determining for what consumers are looking when submitting Internet search queries).

107. The role of web-services companies will depend on how a variety of political and regulatory issues shake out (*e.g.*, whether privacy regulations limit their business models), but I expect a few of these firms to be very successful in this area. Companies that sell advertising based on Internet search and social networks can be expected to make effective use of their ability to help merchants target their advertising in ways that pervasive consumer connectedness will enable. I also believe that web-services providers will extend their success to the business of facilitating targeted offers and customized, context-specific pricing.

108. Will web-services companies be able to use their information as well as their information-collection-and-analysis skills to compete with banks by customizing credit products and conducting superior credit analyses? One issue is whether these companies would be better off selling the information to existing credit card issuers. Another issue is that there is more to life (and success in the payments marketplace) than information processing. As discussed at several points above, at least in the short run trust is a big issue. In my view, at present consumers can be expected to trust several of the largest web-services companies less than they trust their banks and traditional payment card networks.

#### **E. WHAT ABOUT APPLE?**

109. At several points in the discussion above, Apple has been singled out as a possible exception to statements made about broad groups of firms. The future role of Apple Inc. is a big question mark for at least two reasons. First, Apple is uniquely positioned in the mobile

economic ecosystem. It has by far the most powerful consumer brand, and it is the most vertically integrated of any company. Today, Apple is the most successful mobile access device OEM, one of the two most successful mobile OS developers, a web-services company, one of the most innovative and successful bricks-and-mortar retailers, and an online payment company (albeit one that generally rides on top of existing credit and charge card networks<sup>74</sup>). And, in 2006, Apple even filed a patent application for a system under which Apple would be a mobile virtual network operator.<sup>75</sup> Second, Apple has a history of operating closed systems that offer high levels of user convenience coupled with high levels of Apple control.

110. Apple has been conducting research on various wireless payments solutions and has implemented some of them in its retail outlets (e.g., Apple EasyPay, which allows a consumer to use his or her iPhone's camera to scan an item's barcode and then pay using the credit card associated with the user's iTunes account).<sup>76</sup> Will Apple be able to use its powerful brand and vertical integration to create a payment system that it dominates? Or will Apple be driven to be more open in this arena because even Apple will need to work with other enterprises (merchants, if no one else), and these enterprises can see how big a share Apple has taken for digital goods to date?

---

<sup>74</sup> See <http://support.apple.com/kb/HT2001>, site visited April 23, 2012.

<sup>75</sup> AppleInsider Staff, "Filing: Apple conceptualized smart MVNO system ahead of iPhone," *AppleInsider*, April 10, 2008, available at [http://www.appleinsider.com/articles/08/04/10/filing\\_apple\\_conceptualized\\_smart\\_mvno\\_system\\_ahead\\_of\\_iphone.html](http://www.appleinsider.com/articles/08/04/10/filing_apple_conceptualized_smart_mvno_system_ahead_of_iphone.html), site visited May 1, 2012.

<sup>76</sup> See, for example, "Apple Gearing Up for the Coming NFC- iPhone Revolution," *Patently Apple*, April 8, 2010, available at <http://www.patentlyapple.com/patently-apple/2010/04/apple-gearing-up-for-the-coming-nfc-iphone-revolution.html>, and Lance Whitney, "Apple Store's new self-checkout: Nice, but not flawless," *CNET*, November 14, 2011, available at [http://news.cnet.com/8301-13579\\_3-57324198-37/apple-stores-new-self-checkout-nice-but-not-flawless/](http://news.cnet.com/8301-13579_3-57324198-37/apple-stores-new-self-checkout-nice-but-not-flawless/), sites visited January 18, 2012.

**VI. CONCLUSION**

111. I believe that consumers' increasing connectedness via mobile access devices and social networks will lead to evolutionary developments in core payment services but revolutionary changes in services that are built on the information collected through mobile payment services and social networks. I also believe that firms in the telecommunications sector will play a smaller role in payment services than they would like, while traditional payments services providers will play a larger role than many expect. The role of web-services companies will depend on how a variety of political and regulatory issues shake out, but I expect a few of these firms to be very successful in this area. For incumbent payment card networks, the biggest question is whether they have the organizational capabilities to innovate successfully to build on their current strengths of trusted brands and large networks of consumers and merchants. Only time will tell.

**PREPARED STATEMENT OF SARAH JANE HUGHES**UNIVERSITY SCHOLAR AND FELLOW IN COMMERCIAL LAW, MAURER SCHOOL OF LAW,  
UNIVERSITY OF INDIANA

JULY 10, 2012

Mr. Chairman, Ranking Member Shelby, and honorable Members of the Committee, I am pleased to be invited to discuss mobile payments generally, and the benefits and risks that mobile payments offer to merchants and other users in the marketplace.<sup>1</sup>

Mobile payments are among the most innovative payments options emerging across the world. They enable person-to-person and person-to-business payments using flip phones and text messaging (SMS) in less developed countries. In the developed States, where banking systems and telecom networks are more regulated, mobile payments are emerging as a handy means of making small-dollar payments in the person-to-person and person-to-business markets. Perhaps even more importantly in the United States, they are enabling the unbanked and under-banked to make payments at lower risk and cost than some of the other payment options they may have.

Sponsors of mobile payments services vary significantly in size, the breadth and scale of the services offered, and the extent of Federal or State regulation to which their businesses generally, and their payments services in particular, are subjected. Supervision and enforcement also differ significantly.

Mobile payments providers and developers of special mobile payments applications are attracting significant sums in capital investments, which suggest promising business models.

Nationwide merchants such as Starbucks were early adopters of mobile payments options for their businesses. Paying for a coffee or a snack could be completed before the foam on a specialty drink disappeared. Speedier payments, however, can be associated with business decisions to lower security safeguards—at least in the credit and debit industries.

Other merchants in the United States—including plumbers and participants in farm markets and craft shows, and increasingly nonprofit organizations—are beginning to use mobile payments to take payments from their retail customers. These may be small transactions for a pound of field tomatoes, medium-sized transactions for the plumber's house call, or larger payments such as recurring utility, car finance or mortgage payments. But, unlike Starbucks where larger-dollar purchases are probably rare, nonprofit organizations can take contributions or sell quantities of tickets that are much larger in dollar terms using mobile payments options. Small-dollar and larger-dollar transactions may present different risks for merchants, consumers, mobile payments providers, and the financial institutions that hold the funds sent or received via mobile payments.

So far, we have not heard much about larger-dollar payments being made for recurring purposes, such as mortgage payments or car finance installments, but there is little to stop that from happening from a technical or legal perspective. For these types of payments, banks have expressed concerns about the security of underlying banking account information in the hands of relatively new entrants to the payments industry.<sup>2</sup>

Your letter of invitation laid out many possible topics for witnesses to cover. I will focus my remarks on benefits and costs to merchants who take or might take mobile payments, and also to the other regulatory and enforcement issues their participation in payments may present. In some cases, the different issues that consumers and merchants have in the marketplace for mobile payments may converge; on others, they may diverge. I have identified five areas in which mobile payments are likely to benefit our economy and why they are so attractive to merchants, and five areas in which mobile payments present new concerns that may need to be regulated or harmonized and otherwise may require new enforcement approaches. In creating these lists, I made no assumptions about how regulation will evolve.

Turning first to potential benefits of mobile payments, I have five topics to cover and have provided one or more examples to illustrate the range of issues that may arise.

---

<sup>1</sup>My prepared remarks and any remarks I may make in response to your questions reflect only my own views and do not necessarily reflect the views of the Trustees of Indiana University or the Maurer School of Law.

<sup>2</sup>Statement for the Record from Robert C. Hunter, Deputy General Counsel, The Clearing House Association, L.L.C. to The Subcommittee on Financial Institutions and Consumer Credit of the House Committee on Financial Services, June 29, 2012 [hereinafter "The Clearing House Association, June 29, 2012 Letter"].

*1. Taking mobile payments is quick and functional.*

Mobile payments—whether utilizing existing credit or debit card interchange services or “rails” or the services of telecom or other providers—have the potential to help the owners of small businesses, small nonprofit organizations, and farmers and artisans who bring their goods to farmers’ markets and craft shows collect payments from their retail customers.

Mobile payments are speedy; they take only a few seconds to process. They operate without expensive and bulky equipment. They do not require a heavy specialty card reader. (The “reader” for Square, for example, is only about an inch square and the connector fits into the plug on the seller’s smart phone or tablet.) Small merchants using smart phone apps also can take checks from their retail customers, using a feature called “remote deposit.” No doubt, Members of the Committee have seen ads from USAA and other financial institutions for remote deposits for the service members, veterans, and their dependents and families who USAA serves.

In addition, mobile payments, as replacements for magnetic-stripe credit and debit cards, may enable merchants in the United States to skip the impending transition from mag-stripe to chip-and-pin cards and the new readers that chip-and-pin technologies require. Mobile readers may be less expensive than chip-and-pin systems.

*2. Taking mobile payments helps small business owners collect smaller sums due from retail customers and may help to expand the economy.*

Two of the leading mobile payments services providers, Square and Intuit, count among their merchant customers thousands of small business operators (such as plumbers) and nonprofit organizations (who take mobile payments for tickets sales and for contributions from supporters). The less time these merchants have to spend at tellers’ windows or in line for the ATM, the more time they have to help customers, fixing leaking showers or providing services to the community. Thus, mobile payments may help smaller businesses maximize their productivity and add to the economy’s health.

Mobile payments also help merchants at farmers’ markets and craft fairs make sales they otherwise might not—if the consumer involved has to stop and find an ATM machine before completing the purchase.

*3. Taking mobile payments may help merchants deter fraudulent charges at the point of sale.*

At two conferences in which I participated earlier this year, speakers explained in great detail why mobile payments were safer for consumers than payments with traditional plastic credit and debit cards; they paid less attention to whether they would be safer for merchants as well.

Unlike a tangible plastic credit or debit card whose credentialing and verification protocols—the account number, expiration date, customer name, and security code printed on the card itself—remains constant, mobile payments offer a more dynamic set of credentials that includes the mobile device’s location at the time of the payment transaction and the ability of the mobile device to generate a unique identifier for every payment transaction. Dynamic credentialing is one feature that will help merchants—and consumers—avoid fraudulent charges.

Some mobile payments providers such as Square offer merchants another credentialing device—a real-time opportunity to match the face of the person offering to make the mobile payment with the face shown on the mobile device, or with the same merchant’s record of the face of the person who last used the same mobile device to make a payment. Some consumers won’t want merchants to store their photos for later purposes, but many probably won’t care.

In addition, the geolocation of using the mobile device for “proximity” payments adds a security layer. Geolocation gives merchants—as well as processors and providers—an extra level of confidence that the mobile device from which the payment instruction or order is emanating is in fact the proper one.<sup>3</sup>

Dynamic credentialing, including facial recognition possibilities and geolocation information, offers potentially greater safety in payments than the more static tangible plastic cards on which we have relied for the past 35 years or more.

The full-scale dynamic credentialing I have described—without going into detail about the technologies that support it, primarily because they are proprietary technologies in part—may not apply as functionally if the mobile device is being used to make a payment outside of the merchant’s own store. Thus, “remote” mobile payments could raise some of the same fraudulent charge issues that merchants cur-

<sup>3</sup>The degree to which counterfeiting of mobile payments technology becomes an issue is yet unknown.

rently face in “card-not-present” transactions today in the credit and debit card payment spheres.

We do know that the card industry has created a payment application data security standard (PA DSS), much like its relatively successful PCI DSS set of security standards (for payment cards). But PCI DSS is not an ironclad solution to fraud risks from data interception or otherwise, as we learned from the episodes that TJX, Hannaford Brothers, and Global Payments experienced. Each of those companies had been PCI DSS compliant, but none were the nanosecond following the security breaches they suffered. And, once a retailer or processor falls out of compliance, it must reprove its security procedures to qualify again.

4. *Taking mobile payments offers merchants opportunities to build customer loyalty through mobile-based rewards programs, geolocationally based or individually directed advertising, and other information about customers derived from the payment transaction that can be re-used.*

In contrast to traditional tangible plastic credit and debit cards that carry only basic credentialing and payment information, mobile payments offer merchants potential means of communicating with customers that can help merchants build customer loyalty and promote special offers.

5. *Taking mobile payments allows merchants to reach consumers who do not have demand deposit accounts or their equivalents or credit cards.*

With estimates of the number of unbanked adults in the United States upwards of 30 million households [check most recent figure—FTC or FRB March, 2012], merchants who take mobile payments may get customers who otherwise would have to pay in cash.<sup>4</sup> Unbanked consumers, particularly recent immigrants, often have smart phones instead of traditional computers and use smart phones—via mobile payments and mobile banking—to make payments to retailers and creditors.

Unbanked persons’ adoption of mobile payments adoption is a means of reducing their dependence on cash and cash equivalents such as money orders, and may serve as the basis for reducing their costs of participating in the retail economy and reducing the risks associated with carrying cash.

Now turning to possible risks or costs merchants (and consumers) may experience when taking mobile payments, we will see some overlap between risks present in credit and debit card transactions and risks in mobile payments. New risks also may arise.

6. *Taking mobile payments may not be free from interception risks or from malware applied to the data streams along the path maintained by app providers, intermediary processors, and the ultimate payor (such as the financial institution or telecom) that have affected the credit card industry, and thus may pose security risks similar or additional to those in the current payments marketplace.*

Mobile payments providers emphasize the greater security at the point of sale that mobile payments can provide over credit or debit cards, for the reasons I have mentioned above. What is less discussed is a possibility, if not a probability, that because the payments data and accompanying transaction data potentially move through more hands on their path to the ultimate payor, there is a greater likelihood of data interception (through war-driving interception as the data move from the mobile device to the merchant, and from the mobile device to a processor and then to the payor and then to the merchant—depending on the manner in which the payment is processed) or through malware introduced along the path. More simply put, the more participants in payments processing the greater the number of opportunities for interception or the application of malware.

7. *Taking mobile payments and harvesting more consumer information from these payments transactions places more personally identifiable information in the hands of merchants and the payments system participants downstream from merchants—and imposes on them more extensive, and possibly different data-protection responsibilities than they formerly may have had.*

Among the counterweights to the benefits merchants may gain from having more information about their customers and targeted, inexpensive means of communication with them about merchants’ offers, merchants will find compliance responsibilities they may not have anticipated. The more participants in the mobile payments processing path, the greater the number of potential harvesters and holders of personally identifiable information and purchase histories.

<sup>4</sup>Not having to handle cash or checks is a benefit to merchants all of itself in terms of accounting and fraud losses and speeds merchants’ ability to get the proceeds of transactions into their bank accounts and forward to suppliers, landlords, and other creditors.

The value of these data harvests features at least as prominently as the shares of available direct income from marketing the software and processing the payments is likely to offer—at least in the United States where payments processing had been become increasingly efficient (as with checks) or already has been regulated by Congress (debit card interchange and some credit card fee limitations).

Some of these participants are not familiar with Federal and State privacy protections or with requirements of Gramm-Leach-Bliley's Title V (Privacy) and the Federal Safeguards Rule, of the Fair Credit Reporting Act and the Federal Disposal Rule, or with the Children's Online Privacy Protection Act (COPPA)<sup>5</sup> and the COPPA Rule.<sup>6</sup> Some participants will not be covered by either of the first two Acts or rules, but probably are already covered by COPPA and its rule. Having suitable supervision from Federal and State regulators and suitable enforcement resources to protect individuals and this nascent industry from bad publicity is an important goal.

The State of New Jersey recently entered into a settlement with a mobile app creator whose target audience was children.<sup>7</sup> The action, brought in the United States District Court for the District of New Jersey, alleged that 24 x 7 Digital, LLC, and its owners Mark Yamashita and Rei Yoshioka, "collected, maintained, and transmitted to a third party, personal information about children" in violation of COPPA and the COPPA Rule. Among the elements of relief to which the defendants agreed was the destruction of the children's personal information—including the information they transmitted—within five days of the entry of the order.

An additional issue with data collected, stored, and transmitted involves its treatment in a future bankruptcy proceeding of the collector, storage operator, and recipients. The Committee may recall the public furor over the fate of children's data in the early days of Internet commerce involving an online children's toy store and a company called DoubleClick, and the tussle over whether the children's personal information—as part of the debtor's "customer lists" was eligible to be auctioned for the benefit of the debtor's general creditors.

8. *Taking mobile payments does not necessarily relieve merchants of problems with charge-backs for fraudulent charges or other costs associated with data security problems.*

As the Clearing House Association recently explained to the House Committee on Financial Services' Subcommittee on Financial Institutions and Consumer Credit, banks "are usually required to absorb fraud liability and always absorb the cost of recredentialing [the consumer] regardless of whether they had any connection with the underlying breach that compromised the data."<sup>8</sup>

Another aspect of this issue is that merchants will be dealing with more players in the payment than they may be accustomed to, and this broader array of counterparties means more contracts to negotiate and monitor. Contracts will assign settlement times, charge back rules, transactional limits, and costs. Providers may reserve the right to change the terms of these agreements frequently, and may or may not tolerate patterns of behavior that are less than fully compliant with the contracts' provisions. Merchants lose eligibility to participate (as happens upon occasion in the credit and debit payments industries) and have little ability to be restored to participation in their new-found payments tools.

9. *Taking mobile payments does not relieve merchants of responsibility for payment data integrity or for postpayment data security, and, because of the growing number of payments systems participants, may increase time needed to explain payments to customers, increase fraud risks, and also may create new risks for institutions that hold funds and facilitate settlements.*

This heading subsumes two subgroups of issues. The first relates to payment data integrity. Merchants need tools to prevent interference with the data stream so that a payment of \$10 remains a payment of \$10 as it moves through processing.

The second relates to postpayment data security at merchant's own locations and in their databases. Merchants need to safeguard data while the payment is being processed and for whatever time needed to respond to charge-backs, etc. They also need to dispose of the data properly and safely after it is not needed for any particular purpose or ultimately not needed to comply with applicable records retention requirements imposed by Federal or State Governments.

<sup>5</sup> 15 U.S.C. §6501-6506 (2010).

<sup>6</sup> 16 C.F.R. Part 312 (2010).

<sup>7</sup> *Chiesa v. 24 x 7 Digital, LLC, et al.*, Civ. No. 2:12-cv-03402 (Jun. 26, 2012) (consent decree and order for injunction and other relief).

<sup>8</sup> The Clearing House Association, Letter of June 29, 2012, *supra* note 2, at 1, 2, 5.

Data integrity (safeguards against alteration or replication of the sums the consumer intended to pay and the merchant wanted to receive) is important in all payments transactions. We have relatively elaborate rules for checks, credit and debit cards, and funds transfers (wholesale and retail) to protect data integrity and resolve disputes. For consumer transactions with credit and debit cards, Federal law provides error resolution and liability limits.

We also want to provide for postpayment data security. Will the same standards that apply to storage of credit card information post-transaction/payment apply to mobile payments? Will merchants be required to store personally identifiable information related to the purchase separately from the payment transaction information? Will all intermediaries who can collect and maintain data be subject to the same obligations—whether from Federal or State laws?

*10. Taking mobile payments may—but may not—require merchants to adjust their compliance with Federal statutes, regulations, and executive orders pertaining to the deterrence of money laundering or prohibitions against doing business with concerns from designated foreign States or with “specially designated nationals”—individuals who are connected or suspected of being connected with drug or arms trafficking or support of terrorism—for purposes of compliance with the panoply of laws and executive orders enforced by the Department of the Treasury’s Office of Foreign Assets Control.*

I have left for last the law enforcement issues on my list. Mobile payments offer a new set of opportunities to money launderers and those who would fund terrorists. Their person-to-person payments capacities and their speed and ease of transport are factors. Their abilities to disintermediate payments or to layer payments through multiple sets of hands are significant enticements for money launderers. Of these issues, speedy processing/settlements and disintermediation are the most problematic.

These laws are notoriously hard to enforce and preparing compliance plans for businesses eager to comply is a huge industry for law firms and consulting companies. Merchants hate these compliance responsibilities for their complexity and the effort required to train their rotating staffs.

Payments disintermediation generally, and perhaps the more so for mobile payments, is likely to make it harder for Federal agents and local law enforcement to spot problems in local markets. Disintermediation in mobile payments also may hinder enforcement of AML and terrorist-finance control laws and agreements domestically and globally.

Sellers who take mobile payments also may have compliance responsibilities—as will providers and processors—with State safety and soundness registration and examination regimes for money services businesses and with State privacy and data security breach laws.

In closing, I have focused my remarks on domestic transactions and payments in which merchants in the United States and consumers here participate. Cross-border transactions and the payments associated with them raise other issues—issues that add significant dimensions to certain of the issues I have mentioned, with issues pertaining to charge-backs and error-resolution rules at one end of the spectrum, network and device compatibility in the middle, and issues pertaining to taxation and deterrence and identification of money laundering or terrorist support—given the wide array of providers and the technologies or business models they may deploy—at the opposite end.

Banks and consumers are justifiably concerned about broader access to customers’ account information and the enticements that these data present to hackers, and even petty thieves. Consumers are justifiably nervous about the security of any personal information they convey to merchants through mobile devices and their geolocational tracking properties. Consumers are justifiably concerned about who will have access to their personal information and payment account information as it travels, perhaps especially about how much third-party (and Government) access there will be to it.

In terms of the future of regulation of mobile payments, we may see self-regulation, the existing mix of State and Federal regulation and enforcement—or even some regional compacts such as those that spear-headed interstate banking in the 1980s, additional Federal regulation or enforcement, or even a cross-border or multinational regulation and enforcement scheme. A first task is to determine whether the different silos of providers—banks and other financial institutions (as defined by various Federal laws), telecom providers, mobile app developers, and payments intermediaries who are in none of those industries—should be regulated under a common set of expectations and requirements, or should be regulated according to the role they play in mobile payments.

Thank you again for the opportunity to be with you today. If you have questions about this statement or would like to discuss the issues I have discussed further, please contact me.

---

**PREPARED STATEMENT OF THOMAS P. BROWN**

ADJUNCT PROFESSOR, UNIVERSITY OF CALIFORNIA, BERKELEY SCHOOL OF LAW

JULY 10, 2012

Chairman Johnson, Ranking Member Shelby, and Members of the Committee, thank you for inviting me to appear before you today to discuss mobile payments.<sup>1</sup>

Historically, innovation in the payment industry has not been a subject of public interest. I attribute this relative disinterest to the fact that recent innovation in the payment industry has been invisible to consumers. For more than a quarter of a century, the basic mechanics of engaging in a payment transaction have not changed even for payment cards, the newest of our payment technologies: approach point of sale, select card from wallet or purse, hand card to cashier (or swipe the card yourself), and wait for a message that the transaction has been authorized (or declined). Although industry participants can rightly claim that they have radically transformed the process of authorizing the transaction in the past three decades, most consumers don't see it this way.<sup>2</sup>

The phrase "mobile payments" elicits a different reaction. People are genuinely excited about mobile payments. Some of this excitement stems from the eye-popping valuations that some providers of mobile payments have reported to the technology press. But much of it appears to flow from anticipation that the mash-up of mobile with payments will bring a bit of magic to the point of sale. Waving a phone just seems cooler than swiping a plastic card.

Although I look forward to the day when I no longer have to carry plastic or paper to buy things, we should not, in my view, measure the success of mobile payments by the speed with which waving replaces swiping. Existing payment technologies work very well in traditional retail environments. In fact, one might say that they were made for each other. The retail environments that Americans experience most often—multilane retailers, gas stations, quick-service restaurants—were designed to take full advantage of the virtues of existing payment mechanisms (primarily speed at the point of sale). And mobile payment technologies will not soon displace the well entrenched incumbents.

With that said, the bundle of technologies that we generally label "mobile" is rapidly transforming the payment industry. Mobile devices are being turned into Point Of Sale (POS) systems. This is enabling millions of new merchants to accept electronic payments. It is also rapidly changing how existing merchants engage their customers inside and outside of traditional retail environments. These changes hint at the potentially radical ways in which mobile payments will change how people shop, buy, sell, and pay for goods and services. It is possible—though not certain—that mobile payments will further undermine the distinctions between financial services companies, retailers and communications providers. But these really are just hints. At this point, it is impossible to say with any real confidence how mobile payments will affect banks, payment companies, merchants and customers. It is also far too early to pick winners (or losers) among the many mobile payment technologies and companies now emerging.

In my view, lawmakers should be wary of claims that mobile payments need to be further regulated, particularly in the areas of information security and privacy. The payment industry, including the mobile payment piece, is already heavily regulated. New layers of regulation could easily stifle innovation and benefit some providers at the expense of others. And any new laws or regulations directed at the burgeoning mobile payment industry should be developed on the basis of a concrete understanding of the laws and regulations now in place.

With that preface, I will describe the existing regulatory framework for the payment industry, discuss what's truly new about mobile payments, and address potential issues related to consumer privacy and compatibility.

---

<sup>1</sup>I am appearing today in my capacity as an adjunct professor at Berkeley Law School. In my private practice, I have represented and currently represent a number of clients that participate in the mobile payments industry. The opinions expressed in today's testimony are my own and may not represent those of my firm or my clients.

<sup>2</sup>See, Thomas P. Brown, "Keeping Electronic Money Valuable: The Future of Payments and the Role of Public Authorities", in *Moving Money: The Future of Consumer Payments* 127, 132–133 (Robert E. Litan and Martin Neil Baily eds., 2009).

### Existing Regulatory Framework

Participants in the mobile payments space already face substantial costs associated with complying with the existing regulatory regime. Firms that want to enter the business typically confront a choice between obtaining licenses on a State-by-State basis or working under the regulatory authority of a chartered financial institution. And once that threshold is crossed, firms in the payment industry shoulder a long list of compliance obligations.

Generally speaking, a firm that wants to enter the payment business faces a stark choice: find a suitable regulated chartered partner (*i.e.*, a bank or other depository institution) or obtain licenses from all 50 States as a money services provider. The first option brings the mobile payments provider under the indirect supervision of the State and Federal agencies responsible for regulating the chartered partner (*e.g.*, FDIC or OCC). This option also carries costs associated with revenue-sharing and compliance, although some compliance costs and responsibilities may be shared with the chartered partner. The second option brings the mobile payments provider under the direct supervision of various State entities. It also brings with it the initial burden of acquiring State licenses—potentially a multiyear process with associated fees and costs that can easily exceed a million dollars. Annual maintenance costs for State licensing can also be significant.

Beyond this choice, firms in the payment industry must comply with a long list of laws and regulations. Regulation of consumer financial services is complicated. Payments companies—mobile payments included—are typically bound by Federal law providing consumers with recourse in the event of a disputed charge.<sup>3</sup> Firms that rely on a stored value purse to support their payment applications may be required to implement Customer Identification Programs and to report suspicious transactions to the Federal Financial Crimes Enforcement Network (FinCEN).<sup>4</sup> Firms that support international payments must scrutinize their operations for compliance with the requirements laid down by the Office of Foreign Assets Control (OFAC). Firms that store customer bank account or other payment account data are also subject to State laws governing notification to customers and State entities when that personal information is compromised.<sup>5</sup> Finally, although the full scope is still being fleshed out, the Consumer Financial Protection Bureau has supervisory authority over certain “covered persons,” including nonbanks.<sup>6</sup>

One potential way to reduce costs is to eliminate the requirement that an entity must be licensed by all 50 States to operate nationally. There is no apparent benefit, from a prudential standpoint, of such a fragmented regulatory regime. This is not to say that licensing itself has no value—as in the banking industry, some supervision likely helps ensure that mobile payment companies can meet their obligations to consumers. This value becomes diluted, however, when that mobile payments company must contend with the overlapping, but not identical, regulatory requirements across the 50 States. In other contexts, State-regulated entities are able to “passport” a single State license across all 50 States, so that compliance with that individual State’s regulations suffices to allow those entities to do business nationwide.<sup>7</sup>

### Potential Benefit: The Mobile Point of Sale

Although most of the conversation surrounding mobile payments focuses on the possibility of using mobile phones instead of plastic cards to initiate transactions, mobile’s initial impact on the payment industry has been felt on the receiving side of the transaction. Existing forms of payment are mobile at least from the perspective of the consumer (*i.e.*, with rare exceptions, our wallets and purses follow us wherever we go). Until recently, however, electronic payment systems were limited

<sup>3</sup>For example, for mobile payment transactions involving credit cards, Regulation Z, which implements the Federal Truth in Lending Act, limits a cardholder’s liability to \$50 for unauthorized charges. 12 C.F.R. pt. 226.12(c). Likewise, the Federal Electronic Fund Transfer Act provides similar limitations on liability for unauthorized debit card charges. 15 U.S.C. §1693g(a).

<sup>4</sup>All federally regulated banks are required to have a written CIP pursuant to section 326 of the USA PATRIOT Act.

<sup>5</sup>At this time, 46 States, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted such statutes. The National Conference of State Legislatures publishes a comprehensive list, available at <http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx>.

<sup>6</sup>See, 12 U.S.C. §5514(a)(1)(C).

<sup>7</sup>For example, under the Federal Secure and Fair Enforcement for Mortgage Licensing Act (SAFE Act), 12 U.S.C. §5100 *et seq.*, mortgage loan operators enjoy uniform licensing standards nationwide, either through their home States’ participation in the Nationwide Mortgage Licensing System and Registry or by those States’ establishing individual systems that comply with certain Federal standards.

to environments that could be reached by fixed line communication systems. Advances on the mobile front are releasing this constraint.

The transformation of mobile devices into Point Of Sale (POS) systems is taking place on a number of fronts:

- Mobile devices have enabled millions of informal merchants to accept electronic payments. With an app and a small (generally free) device that plugs into the mobile device (known as a “dongle”), artisans, contractors and farmers now accept payment cards from their customers instead of cash.
- Mobile devices are changing how people shop. By equipping sales associates with tablets and smart phones and sending those associates onto the store floor, traditional retailers are turning the entire retail environment into the point of sale. Customers can make purchases in the aisle, rather than waiting to pass through the check-out line.
- Some retailers are using their customers’ mobile devices to extend the point of sale outside the store. They are allowing customers to use their mobile devices to make purchases on their mobile phones (and tablets), go to the store, take the item off the shelf, and walk out of the store without ever having to present a payment card to a sales associate.
- Mobile devices are rapidly changing how people purchase information goods like books, music, movies and software. Again, the mobile device is the point of sale. Consumers use their own tablets and smart phones to access digital market-places, purchase books, songs, apps, *etc.*, and read, listen to and use those goods.

The transformation of the consumer’s mobile device into a primary point of contact between the merchant and the consumer may have a dramatic effect on retail commerce. People tend not to share their mobile devices in the same way that they share laptops and personal computers. This creates the opportunity for merchants to create customized offers for consumers. Most offers currently take the form of discounts, location based offers and fairly basic extensions of traditional loyalty programs (*e.g.*, buy nine coffee drinks and get the tenth free).

This evolution in payment technology may make it possible for restaurants and other small retailers to employ some of the dynamic pricing techniques that have been reserved to large-scale travel businesses. Outside of the travel industry, customers in most retail environments confront a single set of prices. Although different customers may be willing to pay very different prices for essentially the same service, it is difficult for traditional retailers to distinguish one customer from another. As merchants use mobile payment technologies to engage more directly with their customers, they may begin to employ some of the same strategies used by airlines, hotels and car rental companies to maximize traffic in their stores and restaurants, setting lower prices for some customers and higher prices for others. The extension of dynamic pricing strategies from the Nation’s airlines to the corner store may not be universally hailed.

#### **Mobile Payments and Privacy**

In order to customize experiences for particular customers, the merchant (or payment provider) must have access to information about those customers. For example, imagine a restaurant owner trying to craft an offer to attract new customers to her restaurant. Our hypothetical restaurant owner would likely want to reach out to those customers whose spending habits indicate that they like to eat out but who have never eaten at her restaurant. But the restaurateur would likely want to limit the offer to customers who live in the local area, excluding from the scope of the offer tourists and people traveling through the area on businesses. Such distinctions immediately implicate concerns about consumer privacy.

The legal and regulatory framework that governs the collection and use of information regarding consumers is complex and fragmented. Regulatory requirements vary by industry. Financial institutions and affiliated third parties, for example, face one set of requirements under the Gramm-Leach-Bliley Act.<sup>8</sup> Credit reporting companies face another set of requirements under the Fair Credit Reporting Act.<sup>9</sup> Health care providers face another set of requirements under the Health Insurance Portability and Accountability Act’s (HIPAA) Privacy Rule.<sup>10</sup> Federal law also imposes specific restrictions on the sharing of information about certain kinds of pur-

<sup>8</sup> 15 U.S.C. §6801 *et seq.*

<sup>9</sup> 15 U.S.C. §1681 *et seq.*

<sup>10</sup> *See*, HIPAA Privacy Regulations, 45 C.F.R. pt.160.

chases.<sup>11</sup> Special rules apply to certain kinds of information, and the rules can vary depending on the manner in which the information is held at the time of disclosure. Communications in transit receive a different set of protections, for example, than information at rest.<sup>12</sup>

No single agency is responsible for administering Federal privacy law. The FTC has shown the most consistent interest in the subject, though the Department of Justice gets involved, too, particularly when a third party obtains information by illegal means. The prudential agencies have historically been responsible for ensuring that the financial institutions that fall within their purview adhere to the requirements of Gramm-Leach-Bliley. Dodd-Frank has further complicated this picture by severing responsibility for supervising adherence with GLB's privacy requirements from responsibility for supervising adherence to its information security and disposal requirements.<sup>13</sup>

State laws add another level of complexity. A number of States purport to limit the information that can be collected from consumers in connection with certain types of transactions. California law, for example, forbids merchants from, as a condition of sale, requiring or requesting personal identification information from consumers who use a credit card at a point of sale,<sup>14</sup> and the California Supreme Court has defined a zip code to be personal identification information.<sup>15</sup> And, as noted above, 46 States have enacted laws requiring that consumers receive notice if certain information is obtained by a third party.

Private law also plays an important role in this area. The major card networks restrict the uses to which transaction data can be put. Visa's Operating Regulations prohibit a merchant from disclosing a cardholder account number, personal information, or other Visa Transaction Information to any entity other than a registered third party agent, the acquirer, or the acquirer's agent, and that such disclosure must be made for the sole purpose of (i) assisting the merchant in completing the initial merchant transaction, or (ii) as specifically required by law. The payment card networks, through the PCI Council, also regulate how merchants and other participants in the payment card systems may store information related to payment card transactions.

This complex suite of laws does not advance a single policy objective. Much of Federal privacy law is based on the principle that consumers should receive notice and choice with respect to the use of information about them when that information is being used for marketing purposes. As some commentators have observed, it is far from clear that consumers actually want to receive such notices.<sup>16</sup> Other aspects of Federal privacy law are directed at protecting consumers against misuse of data that relates to them. The Do Not Call Registry and the liability caps for unauthorized transactions under Regulation Z and Regulation E fall into this category.<sup>17</sup> Moreover, to the extent that privacy laws attempt to enable consumers to shield their identities from mobile payment providers or other financial institutions, they work at cross purposes with Federal banking law, which as noted above requires firms to collect enough information about their customers to report suspicious transactions.

This complexity should lead lawmakers and regulators to take particular care before creating new laws under the privacy banner. Most efforts to protect consumer privacy interests simply make it more costly for firms to collect information from consumers and to share that information with other firms. But information sharing is not a concern per se, and the focus on sharing tends to distract attention from

<sup>11</sup> For example, information regarding video or video game rental or sale records is protected from disclosure pursuant to the Video Privacy Protection Act, 18 U.S.C. §2710.

<sup>12</sup> "Electronic communications," meaning any transfer of information through electronic means, are generally protected from disclosure under the Federal Electronic Communications Privacy Act (ECPA), 18 U.S.C. §2510 *et seq.*, Title I of the ECPA, known as the Wiretap Act, protects electronic communications while in transit. Title II of the ECPA, known as the Stored Communications Act, protects communications held in electronic storage.

<sup>13</sup> The Dodd-Frank Act amended Title V of the Gramm-Leach-Bliley Act to grant rulemaking authority under Sections 502–509 of that Act to the Consumer Financial Protection Bureau (CFPB).

<sup>14</sup> Cal. Civ. Code, §1747.08(a)(1)-(2).

<sup>15</sup> *Pineda v. Williams-Sonoma Stores, Inc.*, 51 Cal. 4th 524 (2011).

<sup>16</sup> See, e.g., J. Howard Beales, III & Timothy J. Muris, Choice or Consequences: Protecting Privacy in Commercial Information, 75 U. CHI. L. REV. 109, 113 (2008) ("Few consumers actually take the time to read [GLB notices], understand them, and make a conscious choice about whether to opt out of information sharing that is not a matter of statutory right for the financial institution.").

<sup>17</sup> See *id.*, at 118-20 (explaining that the Do Not Call list addressed the problem of unwanted calls at home by focusing on the consequence—the call—rather than access to the information necessary to produce the call—the consumer's phone number).

the problems that give rise to the concern about sharing in the first place—the misuse of sensitive information and the failure to take care against the exposure of sensitive information to malicious third-parties.

### **Compatibility**

This leaves the question of compatibility. Of the issues on today's agenda, this is the most complex and nuanced.

Compatibility (or incompatibility) issues can arise at many different levels. My iPhone is not, for example, compatible with my aunt's Android device. My phone has a different operating system from hers, and it connects to one telecommunication network—Verizon—while hers connects with another—AT&T. My device supports some applications that hers does not. In this sense they are incompatible. But in another sense, they are deeply compatible. Even though the phones are different in many ways, I can use my phone to call or send emails and texts to hers. If we both have accounts with PayPal or Dwolla, I can use my phone to send her money.

As mobile technologies grow in importance as platforms for the exchange of value, compatibility issues are likely to arise. Every mobile payment application may not work in every environment. Starbucks, for example, may choose to keep its mobile payment application separate from that offered by Peet's. But incompatibility issues at that level should not be a source of concern. Indeed, the decision to offer a closed loop payment product may reflect regulatory distinctions as much as anything.<sup>18</sup>

With that said, concerns about the interoperability of different mobile payment applications cannot be dismissed entirely. Both the telecommunications industry and the payment industry have borne witness to significant battles over network access and compatibility.<sup>19</sup> And those issues may surface again. Antitrust authorities in Europe are currently reviewing a proposed payment joint venture in the U.K. in part due to such concerns.

But—and this is a perspective informed as much by my background as an anti-trust lawyer as a student of the payment industry—these issues are sufficiently nuanced that they are not susceptible to a one-size-fits-all solution. Issues of compatibility and interoperability need to be evaluated on a case-by-case basis. Firms may, as in the Starbucks example above, have good reason for rendering their payment applications incompatible with the applications offered by others. But they may not, and in some instances, incompatibility can be a cause for public concern. Fortunately, antitrust law provides a well-developed framework for analyzing these issues as they arise on a case-by-case basis.

### **Conclusion**

This is an exciting time for the payment industry. Emerging technologies are creating opportunities for financial institutions, merchants and consumers to reinvent commerce. This innovation is taking place against the backdrop of a very complex regulatory regime, and although it is possible to imagine ways in which the regulatory burdens facing firms in the area could be reduced (particularly in the area of State-by-State licensing requirements), this emerging industry does not appear to need any new regulation.

Thank you again for inviting me to appear today. I am happy to answer any of the Committee's questions.

<sup>18</sup> See, e.g., 31 C.F.R. pt. 1022 (FinCEN's final rule relating to prepaid access).

<sup>19</sup> See, e.g., *MCI Commc'ns Corp. v. Am. Tel. & Tel.*, 708 F.2d 1081 (7th Cir. 1983); *United States v. Visa U.S.A., Inc.*, 344 F.3d 229 (2d Cir. 2003).