# THE FUTURE OF MONEY: WHERE DO MOBILE PAYMENTS FIT IN THE CURRENT REGULATORY STRUCTURE?

## HEARING

BEFORE THE

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

JUNE 29, 2012

Printed for the use of the Committee on Financial Services

**Serial No. 112–142**

U.S. GOVERNMENT PRINTING OFFICE

76–113 PDF WASHINGTON : 2012

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

HOUSE COMMITTEE ON FINANCIAL SERVICES

SPENCER BACHUS, Alabama, *Chairman*

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

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

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

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

SHELLEY MOORE CAPITO, West Virginia, *Chairman*

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

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

# CONTENTS


Page

Hearing held on:
June 29, 2012 ..... 1
Appendix:
June 29, 2012 ..... 17

WITNESSES

FRIDAY, JUNE 29, 2012

Freis, James H., Jr., Director, the Financial Crimes Enforcement Network (FinCEN), U.S. Department of the Treasury ..... 4
Martin, Stephanie, Associate General Counsel, Board of Governors of the Federal Reserve System ..... 5

APPENDIX

Prepared statements:
Freis, James H., Jr. ..... 18
Martin, Stephanie ..... 32

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Capito, Hon. Shelley Moore:
Written statement of The Clearing House Association L.L.C. ..... 39
Written statement of the Consumer Financial Protection Bureau (CFPB) . 45

# THE FUTURE OF MONEY: WHERE DO MOBILE PAYMENTS FIT IN THE CURRENT REGULATORY STRUCTURE?

**Friday, June 29, 2012**

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

The subcommittee met, pursuant to notice, at 9:30 a.m., in room 2128, Rayburn House Office Building, Hon. Shelley Moore Capito [chairwoman of the subcommittee] presiding.

Members present: Representatives Capito, Renacci, Pearce, Luetkemeyer, Huizenga, Canseco; Maloney, Baca, and Scott.

Also present: Representative Green.

Chairwoman CAPITO. This hearing will come to order. Ranking Member Maloney is on her way, and she said to go ahead and start, so I will start with my opening statement.

First, I want to welcome the witnesses. This morning's hearing marks the final installment in a series of hearings that this subcommittee has had on the future of money. In March, we held a hearing that served as a primer for Members on the current landscape of mobile payments.

Earlier this week, the ranking member and I had a dinner, bipartisan dinner that afforded Members and staff the opportunity to learn more about the different technological developments in mobile payments. And I for one can say it is an exciting future and I wish I had the brain depth to be able to invent some of these things myself.

This morning, we will learn about the current regulatory structure for the payment system and how new developments in mobile payments can fit into this regulatory structure.

The past decade has seen tremendous growth and innovation to technology that will no doubt influence the payment system in this Nation and abroad. We can't really imagine what the technology may be 6 years from now. For that reason, it is important for this committee to understand the rules of the road for mobile payments. Does today's regulatory structure provide seamless protection for consumers, easy dispute resolution, and protect against money laundering and the financing of terrorism, or do we need to make changes and, if so, what changes should be made, minor or major?

This morning, we have two very important voices to talk about today's regulatory structure. The Federal Reserve has been the ex-

pert on the payment system for a long time and the Boston and Atlanta Feds combined to do much of the best early examination of the promise and potential pitfalls of mobile payments.

While their consumer protection duties were transferred to the Consumer Financial Protection Bureau (CFPB) 2 years ago, the Fed will continue to be an important player. As witnesses at our first mobile payment hearing warned, some of the forms of payment available, including those tied to phone bill billings, may not fall under current payment law as we understand it.

Meanwhile, the Treasury's Financial Crimes Enforcement Network, or FinCEN, prescribes the regulations that help our law enforcement agencies fight money laundering and the financing of terrorism and is in the best position to tell us if any parts of the newer forms of payment might fall outside of our current requirements for financial institutions to report suspicious activities. We need to make certain we get this latter part right. A senior economist at the World Bank has warned explicitly that it would be much harder to follow the future of money and to establish the sender and receiver of money as the transactions move towards anonymity.

We also have, and I will ask for unanimous consent to insert into the record, a statement from the CFPB. Also, I want to thank both of our witnesses for their work that they have done in preparing for today's hearing and for their years of steady government service. In particular, the committee would like to thank Director Freis for his more than 5-year service as head of FinCEN. That is the longest tenure of anyone in what we know is a very difficult job. We are aware that you are transitioning to another job and could have declined this invitation to testify, so we especially want to thank you for coming today.

Mrs. MALONEY. Good morning.

Chairwoman CAPITO. There she is. I thought I heard her coming in.

Mrs. MALONEY. I apologize, but we had a Democratic Caucus meeting on health care.

Chairwoman CAPITO. I recognize the ranking member.

Mrs. MALONEY. I want to thank so much the chairwoman, and welcome the Federal Reserve and FinCEN. This is our third look at the issue of mobile payments, and I have to commend the chairwoman and the committee for holding this series of hearings on this new technology, and literally, we have cohosted a dinner to look at it and expose the new technology to Members of Congress. We saw this earlier in the week and I am pleased that we are trying to get out ahead of the issues rather than finding ourselves reacting but not being proactive.

I really think that I would like to put my opening statement in the record. Believe me, it is very interesting, but I would like to hear the testimony today and have the opportunity to ask questions, particularly in the area of identity and security and maintaining the security of consumers with these new products.

Thank you. I yield back.

Chairwoman CAPITO. I now recognize Mr. Canseco for 2 minutes.

Mr. CANSECO. Thank you, Madam Chairwoman. The growth of the mobile payment industry represents a tremendous opportunity

for everyone, from consumers and merchants to financial institutions and other providers. Mobile payments have already proven to be the most significant development in consumer payment methods since the move away from checks to debit cards. This should bring a great number of benefits, particularly in the form of competition and lower costs for consumers.

Yet, it is essential that policymakers and regulators structure a regulatory framework that helps protect the private information of mobile users, but also encourages investment and innovation within the industry.

It is very relevant to mention that the last significant policy initiative in this area, which was price fixing in the debit card market, was the exact opposite of what Congress and regulators should be doing, and I hope we have learned from that very significant mistake.

And so, Madam Chairwoman, my hope is that today's hearing helps Congress and regulators embrace these new innovations and that it leads to a properly constructed regulatory framework that works for everybody involved.

I yield back.

Chairwoman CAPITO. The gentleman yields back.

Mr. Scott for 3 minutes.

Mr. SCOTT. Thank you very much, Madam Chairwoman. Let me commend you and the ranking member for putting this very important and timely hearing together. Certainly, nothing could be more timely than the rapid advancement of technology. No area is that more profound than the mobile phones we use. We basically have become pleasantly captive to the cell phone. And we need to make sure that the American people are adequately protected from abuses from invasions of identification theft.

Many people may not know this, but 92 percent all the American people now use mobile phones. The pay phone has gone by the way. And with that comes all other types of services that are connected with it. Many times people have their bank accounts, their bank statements on their mobile phones. They have medical information, pharmaceutical information, and prescription drug information all on their phones. It has become an integral part of our physical beings.

And so, we really have to make sure that adequate protections are there, and half of these phones are what we call Smartphones, which are capable of processing mobile payments, credit card payments. So when you look at the entire scope of the significant amount of impact that mobile phones have on our entire existence, particularly very vital and pertinent information regarding our financial accounts, our health care, all very important issues, it is very important that we make sure that proper regulations are in place to protect the American people, and I look forward to hearing the panel.

Thank you, Madam Chairwoman.

Chairwoman CAPITO. Thank you, Mr. Scott. With that, I believe opening statements are completed, and I would like to turn to the panel. Our first presenter is Mr. James H. Freis, Jr., Director of the Financial Crimes Enforcement Network (FinCEN) at the Department of the Treasury. Welcome.

**STATEMENT OF JAMES H. FREIS, JR., DIRECTOR, THE FINANCIAL CRIMES ENFORCEMENT NETWORK (FINCEN), U.S. DEPARTMENT OF THE TREASURY**

Mr. FREIS. Thank you, and good morning, Chairwoman Capito and Ranking Member Maloney.

I am Jim Freis, Director of FinCEN, and I am pleased to be here today to discuss FinCEN's efforts to establish a meaningful regulatory framework for mobile payments and other emerging payments methods. My testimony today will focus on some of the most important regulatory and analytical work being done to prevent criminal abuse of the financial system as technological advances create innovative ways to move money.

At the outset, I would like to make a distinction between mobile banking and mobile payments. Mobile banking involves communication and direction from an account holder about their account at a depository institution. Mobile payments essentially involve the direction of funds outside of a bank account to effect payments or other transfers. Let me emphasize that both types of activity are subject to relevant FinCEN regulations for anti-money laundering and counterterrorist financing purposes, either as part of the requirements on banks or as part of the requirements on money transmitters.

Recognizing that payment systems evolve rapidly, FinCEN took a comprehensive approach in this area, revising its regulations 1 year ago specifically to cover mobile payments and other innovations. The rule was developed to be technologically neutral and hopefully cover new developments for years to come. Specifically, the rule focuses more on the underlying activity as opposed to the particular electronic communication vehicle. If a mobile phone allows person-to-person payments or payments that cross borders in or out of the country, then the provider must identify the customer, keep records of transactions, and have procedures in place to report to FinCEN possible money laundering or other suspicious activity.

In furtherance of that, FinCEN's regulations make it clear that the acceptance of funds from one person and then the transmission of those funds to another person or location by any means constitutes money transmission and that any person doing business in whole or in part in the United States who engages in money transmission, regardless of other business lines such as telecommunication services, would likely be a money services business subject to FinCEN's regulations, and as such must register and comply with all requirements applicable to a money transmitter.

Shortly after publication last year of the final prepaid access regulation, and as part of FinCEN's commitment to engage in dialogue with the industries we regulate, FinCEN held a series of town hall meetings with representatives from the prepaid access industry. FinCEN has already released a number of pieces of guidance with respect to the prepaid access regulation, and we anticipate that additional guidance will be forthcoming related to some of the issues raised by industry attendees during those town halls, as well as ongoing requests for clarification and guidance on the new regulatory framework.

I would like now to briefly mention some of FinCEN's analytical work in the mobile payment space. As part of our ongoing support

to law enforcement, FinCEN regularly provides reference manuals to help better understand the workings of various payment mechanisms and to provide steps to utilize its understanding in specific criminal investigations. One recent such manual focused on mobile payments. In preparing the manual, and in subsequent law enforcement outreach, we have seen an interesting trend in the mobile payments industry where different telecommunication systems and financial mechanisms merge and become interwoven in the same overall mobile payments transaction.

For example, a customer might choose to initiate a remittance to a physical money service business location, with the transaction then being processed through the MSB's internal system, the payment of the funds then going to a recipients mobile account. Upon completion of the transaction, the recipient typically receives a text message notification on their mobile phone that indicates the funds have been credited to their mobile account.

This transactional overlap results in multiple informational chokepoints that may assist law enforcement's efforts to follow the money trails and identify other accounts and transactions associated with a given subject. Fortunately, FinCEN's prepaid access regulation was specifically designed to be flexible and to accommodate new technologies as they emerge, but also to capture innovative payment methods currently being used by U.S. institutions such as aspects of the scenario I just described.

In the area of new payments methods, the Administration has made appropriate oversight of prepaid access products a priority, and FinCEN is very encouraged by the progress we have made thus far. Moving forward, we are dedicated to continuing to build on these accomplishments as we encourage legitimate consumer and commercial activity to flourish, but also help financial services providers to focus on serving their customers, not criminals.

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

[The prepared statement of Director Freis can be found on page 18 of the appendix.]

Chairwoman CAPITO. Thank you, Director Freis.

We will now hear from Ms. Stephanie Martin, who is Associate General Counsel for the Federal Reserve Board of Governors. Welcome.

**STATEMENT OF STEPHANIE MARTIN, ASSOCIATE GENERAL COUNSEL, BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM**

Ms. MARTIN. Thank you, Chairwoman Capito, Ranking Member Maloney, and members of the subcommittee. Thank you for inviting me to appear before you today to talk about the regulation of mobile payments.

The evolution of technologies that enable consumers to conduct financial transactions using mobile devices has the potential to affect their financial lives in important and new ways, including by expanding access to mainstream financial services to segments of the population who are currently unbanked or underbanked. But with any payment system, including a mobile payment system, regulators have two key concerns: one, whether consumers are pro-

tected if something goes wrong such as an unauthorized transaction; and two, whether the system provides appropriate security and confidentiality for the transmission and the storage of payment instructions and the personal financial information of consumers.

In many mobile payments, at least some parts of the transaction are settled through existing payment systems, such as card networks, and are subject to the statutes, rules or procedures that are already in place. The evolving aspects of mobile payments typically are related to new consumer interfaces and new payments or settlement arrangements which can involve service providers that have not traditionally been in the payments business, for example, a telephone company.

Making payments through nontraditional arrangements may change the legal protections related to the purchase, depending on the details of the arrangement and the applicable statutes and rules.

There is a legal framework to address the payment activities of banks, and Federal bank regulators have the tools to ensure that banks offer mobile payment services in compliance with the consumer protection provisions of any applicable laws or rules, such as the Electronic Fund Transfer Act (EFTA). The application of most Federal consumer laws to mobile payment transactions is subject to the rulemaking and interpretive authority of the Consumer Financial Protection Bureau.

As part of the supervisory process, the banking agencies review bank security protections for new payment interfaces, as well as for compliance with rules on information security, identity theft prevention, and anti-money laundering.

Many of the questions that have arisen with respect to mobile payments, however, relate to the involvement of nonbanks. Nonbanks can have a variety of roles in a transaction, such as an agent of a bank, a manager of a prepaid value program, a money transmitter or a company that bills customers for payment transactions. The applicability of existing consumer protection laws or security requirements to nonbanks generally depends on the nonbank's role in the mobile payment and the specific provisions of a particular statute.

In conclusion, it is difficult to make broad generalizations about the applicability of existing statutes and rules to mobile payments. This is due to the different types of service providers, bank and nonbank, the wide variety of payment arrangements and the potential applicability of both banking and nonbanking laws to any given arrangement. Given recent technological developments in mobile payments, further analysis of the adequacy of existing laws may be appropriate in order to ensure that consumers are adequately protected.

At the same time, 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 would not stifle the very innovations that would benefit consumers overall.

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

[The prepared statement of Associate General Counsel Martin can be found on page 32 of the appendix.]

Chairwoman CAPITO. I want to thank you both and I will begin with my 5 minutes of questioning. I would like to make a comment on something, Ms. Martin, you said at the end of your statement, because of the dinner that we had last night, I think we had five presenters who had a whole range of forward-thinking mobile payments, some that are currently in the system, some that are innovating into the system. And one of the concerns that they have and I think we share the concern and you did through your comments is that we don't get ahead of the curve here regulatorily, with regulation, and stifle the innovation and cut off what could be an ease of payment, bringing in people who are not in the bank or underbanked. And so, the point of this hearing is to really see where are we and where do we need to be, not so much where do we as lawmakers need to come in and clamp down. I don't think that is an issue, but I think it is something to keep our eye on.

I would like to ask a general question. Are there in existence now informal or formal agreements between banks on the mobile payments issues? Is this a structure that banks have formally recognized through specific agreement along the lines of mobile payment and conflicted consumer protections that are contained within or does it fall within just a general—

Ms. MARTIN. I would say for particular new arrangements that are using new technologies, usually you see a partnership. Often, you see a partnership between a bank and a nonbank service provider, sometimes the telephone company would be involved. So in a particular mobile payment arrangement, they would have contracts and agreements in place as to how that will work. But many of these arrangements ultimately get funding (into a mobile wallet, for example), using existing, I will call them, "payment rails." So a consumer with a virtual wallet who wants to put in that wallet a credit card or debit card would be funding those credit or debit card transactions through the normal card networks.

Chairwoman CAPITO. Existing.

Ms. MARTIN. Those arrangements and agreements and rules are already in place. Is that responsive to your—

Chairwoman CAPITO. Yes. I don't know if you have a comment on that, if you are aware, and certainly at FinCEN, you are looking internationally, too. Are there specialized agreements for mobile payments that you are aware of or do they just fall within the normal bank-to-bank relationship agreements that are already existing?

Mr. FREIS. I would concur with Ms. Martin that if you are trying to transfer between different financial institutions, then it is largely today reliant on existing bank centric networks such as those involving what we commonly know as your MasterCard or Visa card for which you need a bank to be an issuer of that card relationship. Otherwise, you are talking about proprietary systems, so I am going to a specific money transmitter and I must be a member of that network.

Chairwoman CAPITO. Let me ask you this, too, in your statement you were talking about nonbank participants in mobile payment, and one of the innovators that we saw was talking about being able

to have a card that you could swap between paying with your Visa debit, for example, or maybe your rewards points. That would be something that really wouldn't be covered, because that would really be a vendor. Let's say you would be using your USAir frequent flier miles or something of that nature. Is that something that you all have taken into consideration or are looking at? Do you understand what I am asking?

Ms. MARTIN. I understand that you could have a mobile wallet arrangement where you can choose different ways of paying for whatever you are purchasing.

Chairwoman CAPITO. Right.

Ms. MARTIN. And today you have a credit card with flight miles on it that is usually redeemable at a specific merchant. So I can use my US Air flight miles at USAir. That is typically within a very proprietary system. But if I were to use my debit card, then I would have to go get the money from my bank account, so that would move over payment card network rails. I think it is going to depend on what card you pull out of your virtual wallet as to what rails that transaction will follow.

Chairwoman CAPITO. Right. I think the important thing on that is the consumer protection jurisdictions and are they covering all sorts of different transactions that may be coming over the same virtual wallet.

Ms. MARTIN. Right. I think one of the issues is to look at the consumer protection laws such as the EFTA and TILA. If is there a credit card involved, it is the CFPB that is going to have the rule-writing authority under those laws. But it is not clear that those laws do apply in each case where a nonbank is involved.

Chairwoman CAPITO. Right. I think that is the point you were making.

Ms. MARTIN. Yes. In some cases, those laws were really written with a bank-type relationship in mind. And those concepts may or may not apply, depending upon what the nonbank's role is and how the system is structured.

Chairwoman CAPITO. Thank you. Ms. Maloney?

Mrs. MALONEY. First of all, I want to thank both of the panelists today for your testimony, and I agree with the chairwoman that we certainly do not want to stifle innovation, which was part of your testimony, Ms. Martin, as we move forward to make sure that consumers are protected and that money laundering is prevented and that other things are in place.

As you look at this evolving new technology, I must say in terms of privacy and consumer protection, some of the technology really identified the person by their voice, by a photograph, very detailed ID that would be hard for someone to steal your identity, which is regrettably a growing crime in America among many of our constituents. I would like to get a sense from you because this is not necessarily a bank, it is not necessarily—it is like new. Who do you think would be the primary regulator? Someone has to be in charge. Which agency should take the prime role over mobile payments which are not necessarily bank products? And to what extent should the banking regulators be involved and coordinate? And who do you see as taking the form of the primary regulator, the FCC, the FTC, the CFPB, the Federal Reserve, Treasury?

Your comments first, Mr. Freis, and then Ms. Martin. How do you see this being regulated? We have to have someone to call if there is a problem.

Mr. FREIS. Yes. Thank you for your question. From my perspective at FinCEN, we have a great deal of experience in working with a range of different financial service providers and a range of different agencies to ensure appropriate regulation. So for the anti-money laundering counterterrorist financing purposes, the principle is any way that you can move money, any way that you can intermediate value can be abused by a criminal actor. So that is the reason why FinCEN looks at this aspect centrally. In the example that I have given whether a money transmission is made through a bank, whether it is made through a traditional money services business or through new providers such as in the mobile payment space we have a common interest in making sure that we have done as much as possible to mitigate the risk of criminal abuse.

In so doing, we rely on the Federal banking agencies or State regulators and money transmission space, and we found that is an important working model just as we do in other areas such as insurance, working with the States or with the SEC working in the securities industry. Each of them will have a primary responsibility with respect to whether it is safety and soundness, consumer protection, but our ability to work with them is on our single mission of the anti-money laundering requirements, I think it is central to avoiding the regulatory gaps and the balances they must take that criminals frankly would abuse. So I think the model we have, at least for my purposes, is working.

Mrs. MALONEY. And Ms. Martin?

Ms. MARTIN. I agree basically with what Jim said. I think it is an interesting strategic question to think about what agency should take ownership of this area. It is such a broad area and it covers so many different types of entities, it is really hard to point to one agency with the right experience and expertise that can cover the gamut. So at least as a first step, it certainly seems to me that there should be coordination and consultation among all of the agencies you named, as well as FinCEN and State regulators, to figure out who has what, who is covering what bases, and what gaps there are that need to be addressed. And I think you can achieve consistent results in that way through interagency discussion and coordination.

Mrs. MALONEY. That is true, but finally someone has to be in charge. Otherwise, everyone is pointing fingers at each other, but building on your question or the statement that you had, they were testifying to us or telling us at this dinner we had exploring the new technologies that they are out there now, tens of thousands of people are already using these products. And so, I wanted to know what protections have States or actions have States put in place to protect consumers from unauthorized transactions and disputed charges to prepaid phone deposits or wireless phone bills? I am wondering what actions States have taken, if any, in this area?

Ms. MARTIN. States do have money transmitter laws, where if the entity meets the definition of money transmitter, many States

have registration requirements and some bonding and investment limitations. To that extent, I know States do have some laws.

When you talk about bringing phone companies into the equation, perhaps that is something we might want the FCC to weigh in on. I am not sure what kinds of protections exist in telecommunications law for consumers who are billed for particular line items on their bill which might represent a payment. I think that is worth some further investigation.

Mrs. MALONEY. My time is up. Thank you, Madam Chairwoman.

Chairwoman CAPITO. Thank you.

Mr. Canseco?

Mr. CANSECO. Thank you, Madam Chairwoman. Ms. Martin, we often talk about the unbanked in our country. It is noted that 10 percent of mobile payment users don't have a bank account and that roughly 30 million Americans are either unbanked or underbanked. So how do you feel the growth of mobile payments will affect this group and would they be more or less likely to enter the banking system?

Ms. MARTIN. It is hard to predict the second question that you asked. I think mobile payments present a good opportunity for the banked and unbanked to obtain payments services perhaps that are more efficient and perhaps even cheaper than what their alternatives are today, which may be going to a check casher or a money transmitter and paying pretty hefty fees. It is also very convenient. As you stated or somebody stated, over 90 percent of people do have a mobile phone, so it is a very ready device for them to enter into the financial system.

To the extent that banks can offer products that are available through that mechanism, that might be a way to get people into a bank relationship through a mobile phone that is a replacement for a check casher or buying a money order.

Mr. CANSECO. One concern, Ms. Martin, that I have is that we adopt a regulatory framework that makes it more costly and more prohibitive for market participants to innovate within the space. What specific steps should regulators be taking to encourage innovation and investment in the mobile payments space while also ensuring that data security and enforcement of anti-money laundering laws are working?

Ms. MARTIN. Yes, the walk on the fine line between regulation and not stifling innovation is always a tricky one. I think it is important for regulators to set some priorities and some key concerns that you would like to see addressed in these mobile payment arrangements regardless of how they are structured. I mentioned a couple in my testimony; one basic consumer protection is security. You might add anti-money laundering to that list. So if we can look across all of these arrangements and make sure that those key concerns are met, then maybe you don't want to drill down into more detailed requirements until you see where the market is going to come out. So allow people to experiment, innovate with pilot programs until some industry best practices are established. And then, that might be a time where you see particular patterns emerging that you think you should address with more regulation. That might be the time to do that.

Mr. CANSECO. Thank you. This next question goes both to you, Mr. Freis, and Ms. Martin. Do you believe that international standards should apply to mobile payments? And if so, what type of coordination is going on between regulators in the United States and other countries?

Mr. FREIS. I am happy to address that first. With respect to our anti-money laundering counterterrorist financing efforts, we have developed international principles in terms of expectations as to what the risks are and efforts are to mitigate them. We do that at a broad level in terms of different products area, including money transmission, not things that are specific to the device of mobile payments as opposed to other mechanisms for entering the system, and I believe that is the right approach, especially based on the concern that you just expressed about rapidly evolving technology. It is better for us to define the risk and expectations of how to mitigate them and not to prescribe one specific area.

By the time we had agreed on any international basis, it would already be obsolete in terms of technological advances. That is being done on an international basis in particular through the Financial Action Task Force. The United States has been very active in guiding those developments and pushing other countries to work in that area. I can tell you in my own work in the development of these prepaid access regulations, specifically including mobile phones as I have described in my testimony, I very actively engaged with my counterparts, both the regulatory side and the law enforcement support side, throughout the entirety of this process, sending them copies of the documents when we put them out for public notice and comment, seeking from them examples of specific cases where they might have seen law enforcement abuse to make sure we were addressing those specific concerns.

Mr. CANSECO. Thank you, sir. Ms. Martin?

Ms. MARTIN. I would agree with that and also add that it seems to me that this type of service is so new and rapidly evolving that it is a bit early at this point to start thinking about international regulatory standards. Generally, those kinds of discussions come when systems are more mature and principles and best practices have been established, and that really hasn't happened yet.

Mr. CANSECO. But we need to start thinking about this.

Ms. MARTIN. Oh, yes, I do agree with that.

Mr. CANSECO. Thank you very much. I see that my time has expired.

Chairwoman CAPITO. Thank you. I would like to ask for unanimous consent to insert 2 statements into the record: one from the CFPB; and one from The Clearing House Association. Without objection, it is so ordered.

I now recognize Mr. Baca for 5 minutes for questioning.

Mr. BACA. Thank you, Madam Chairwoman, and Ranking Member Maloney for calling this meeting, and I thank the witnesses for being here this morning.

One of the basic goals in reviewing this topic is ensuring that the consumers understand the product. I think it is very important that they understand the product they are using and the risk involved. With the advancement of technology, we have seen security threats grow as well. When it comes to electronic payments specifi-

cally in identification, theft is a real concern to a lot of us. What recourse do consumers have when they encounter problems with unauthorized charges or the amount they are charged is inaccurate? That is a common problem that we have, especially people who take advantage of a lot of our seniors, and seniors are the ones most vulnerable for this kind of problem, even though they get involved in this technology.

I open it up for either one of you to respond.

Ms. MARTIN. To the extent a mobile payment results in a debit through a checking account or a charge to a credit line that is covered by the EFTA or TILA, both have error resolution procedures which would kick in for consumers.

Mr. BACA. How would they be informed, because they may be covered but they want to recoup their money and that is part of the problem. What is the time in delay between the time something occurs and the time that their account is reimbursed, because that means money lost, and a lot of them are on a fixed income?

Ms. MARTIN. Right. Under EFTA, the existing timeframes are set forth in the statute and should be disclosed to consumers in the bank disclosures as well. I believe an investigation has to take place within 10 days. If the investigation is not concluded by that time, the consumer has to be reimbursed while the investigation continues. But in many cases, it gets concluded before 10 days are up.

Mr. BACA. Would the consumer be informed of the process of what is going on within that period of time?

Ms. MARTIN. I can get back to you on that.

Mr. BACA. If they don't know, they don't know you are doing anything—

Ms. MARTIN. The consumer initiates the process, and then they should be advised of what the process is.

Mr. BACA. "Should be" and "doing it" are two different things.

Ms. MARTIN. The other point that I wanted to make is that it is not clear that those laws apply in all cases where a nonbank is involved. I do know that some nonbank payment providers have incorporated Reg E, EFTA-like, error resolution procedures into their rules and their user agreements. It is not quite the same thing as having those error resolution procedures applied to them by rule, but they are trying to use those procedures within their own arrangements.

Mr. BACA. Okay. Let me ask another question, along these same lines. Consumers sometimes find miscellaneous or added charges tacked onto their monthly bills. We used to see this a lot with credit cards. Obviously, this has caused a lot of consumers to dispute charges. How consistent are the mobile payments dispute resolutions policies of the various wireless providers? And should Federal regulators pursue a minimal national standard?

Ms. MARTIN. The wireless provider consumer dispute resolution process would be something I think that the FCC would weigh in on. That is really outside my area of expertise or knowledge. That would have to do with if you get billed on your phone bill for a payment that is wrong, what are your rights? And I think that merits some further investigation and fact-finding.

Mr. BACA. And then consumers have expressed concern with practice—oh, my time has expired. I am sorry.

Chairwoman CAPITO. You actually have 58 seconds left, but we have just been called for a vote, so I am going to go to Mr. Luetkemeyer because he is the next questioner. And then when he completes his call, we will decide what the will of the committee is if we want to come back. We have two votes.

Mr. LUETKEMEYER. Thank you, Madam Chairwoman. And thank you for the briefing the other night on mobile payment systems. It was quite instructional, and after the meeting I told my staff that I am going to have to get rid of my rotary phone and get in the 21st Century here.

So thank you for being here this morning and I have just a quick couple of follow-up questions relating to what my colleague, Mr. Canseco here, asked with regard to international standards. Ms. Martin, you made the comment that you are going to wait until the market is mature before you actually get into the middle of a regulatory promulgation here and that is kind of after the horse is out the door if you are going to take that approach. I would think you would want to work with those entities that are producing these new innovations and find ways to curtail abuses of those right off the bat. I was surprised at that comment.

Ms. MARTIN. My remark there was directed specifically towards international standards.

Mr. LUETKEMEYER. International standards are what I am concerned about.

Ms. MARTIN. Generally when we work on international standards in other contexts, this occurs when we have some rules and thoughts in place about how that market is regulated here. All I am saying is that I think we need to do further investigation domestically before we start talking internationally.

Mr. LUETKEMEYER. Are you familiar with the CFPB's proposed rule dealing with international wire transfer services?

Ms. MARTIN. I didn't hear the first part.

Mr. LUETKEMEYER. Are you familiar with CFPB's proposed rule dealing with international wire transfer services?

Ms. MARTIN. The remittance rule?

Mr. LUETKEMEYER. Yes.

Ms. MARTIN. I am somewhat familiar with it.

Mr. LUETKEMEYER. Okay. Are you for it, against it, think it is going to work? How is it going to affect mobile payments, I guess is the question?

Ms. MARTIN. That is a good question. I am not sure there are any mobile payment arrangements at this time—and maybe, Jim, you can jump in here—that are being used for international remittances.

Mr. FREIS. Actually, there are some services for which mobile payments are a part of that international remittance network, as I have mentioned in my written testimony, but that are covered from our regulatory framework. And, Congressman, responding to your question, I just wanted to reiterate that we at FinCEN recognize the risks of cross-border payments, and it is for that purpose that although some of our regulations are subject to thresholds or some activity test, any ability to transfer money in or out of the

country from a zero dollar threshold automatically brings that payment mechanism, including that mobile phone network, into our regulatory framework and subject to all of those controls.

And furthermore, one of the risks that we had concern with is that if we impose an important regulatory framework on the United States but do not do something with the ability of entities from outside the country to access, that would pose a vulnerability. So we specifically have also amended our regulatory framework last year taking advantage of the full authority that Congress gave to us to assert jurisdiction over foreign-based money transmitter providers to the extent that they are serving U.S. persons. So that also should avoid that type of regulatory arbitrage, people from outside the United States.

Mr. LUETKEMEYER. There were a couple of studies that had been done. The Atlanta Fed, Swift, and the World Bank have acknowledged that these new services had a potential to facilitate money laundering. And, the Swift study recommends that regulators take a proportionate approach, limited amounts that can be transferred, advanced financial inclusion and ensure the soundness of financial services.

What are your thoughts on those recommendations or are you aware of those?

Mr. FREIS. Yes, I am, and it is exactly those type of considerations that we took into account in the development and promulgation of this final rule last year, and we will continue to monitor. One thing I can say is that something I instituted after joining the agency more than 5 years ago is a year after we promulgate a new rule, we take a look at whether it is achieving its intended effect and then reconsider whether changes are made. That is something we will constantly look at and will certainly be doing in this area in a very rapidly evolving marketplace.

Mr. LUETKEMEYER. Thank you. I yield back the balance of my time. Thank you, Madam Chairwoman.

Chairwoman CAPITO. Our final questioner will be Mr. Scott, and I think then we will dismiss the panel. We have about 10 minutes left until votes.

Mr. SCOTT. Thank you, Madam Chairwoman. Let me just ask you this: What advice would you give the American people if one of them were to lose their cell phone, their mobile phone? What should they do, especially regarding how they protect their vital information? What should they do if they lose their cell phone?

Ms. MARTIN. I would say two things, and one is, before you lose your cell phone, make sure you have a password on it.

Mr. SCOTT. I am sorry, you said, "password?"

Ms. MARTIN. Password-protect your cell phone. Also, I think it is very important for consumers to understand what is on their phone and who to call if they lose their phone. So to have that information somewhere other than on your phone would be a very good step in helping you mitigate the problems that could occur if you lose your cell phone.

Mr. SCOTT. Okay. But on your side of things, what steps would you as regulators take to make sure consumers know how and when and where to complain, to call, what do they do? It is good that they put their cell phone, their ID and password and all of

that, but is there anything specifically they should do? Should they just forget it? If for example, I lose my credit card, I am going to call somebody and I am going to say, stop payment on that. So there ought to be something or some procedure we can communicate to the consumer as to what you do, particularly if that consumer may not have the password on it or they may have—some scam artists out there now are capable of doing a lot of things with this advance in technology. So if we don't have a procedure for what consumers should do, we ought to get something out so consumers will know how, when, where, and who to contact once they lose this precious instrument.

Ms. MARTIN. I think who you call might depend on what kinds of mobile payment applications you have on your phone. If I had a mobile wallet with a credit card attached to it, I would do exactly the same thing as if I lost my plastic; I would call that credit card company. I think many of those procedures that you would follow if you lost your real wallet would be the same things you would do if you lost your phone.

Mr. SCOTT. Okay. Mr. Freis, do you have any comment on that? What advice would you give consumers?

Mr. FREIS. I think being aware of the risk is clear. One thing that must be said is that part of the reason why these payment products, these prepaid whether it is through a mobile phone or a card have taken off because do you have recourse to your funds. So unlike if you lost your wallet with cash in it, if you have lost a card, you do have the ability to contact the provider to shut down that old card and get your money back. It is not lost for good. So it is exactly that, which has been of benefit to consumers, and I agree with you that it is important that they understand these steps to take to follow to get the funds back such as Ms. Martin described.

Mr. SCOTT. Thank you, Madam Chairwoman.

Chairwoman CAPITO. Thank you. With us being on a vote, and no further questions, the Chair notes that some Members may have additional questions for this panel, which they may wish to submit in writing. Without objection, the hearing record will remain open for 30 days for Members to submit written questions to these witnesses and to place their responses in the record.

I appreciate the witnesses coming today, and I know we will have many more discussions on this as the evolving technology brings different challenges, but also different opportunities, and I appreciate that. This hearing is adjourned.

[Whereupon, at 10:28 a.m., the hearing was adjourned.]

# A P P E N D I X

June 29, 2012

**Statement of James H. Freis, Jr., Director**
**Financial Crimes Enforcement Network**
**United States Department of the Treasury**

**Before the United States House of Representatives**
**Committee on Financial Services**
**Subcommittee on Financial Institutions and Consumer Credit**

**JUNE 29, 2012**

Chairwoman Capito, Ranking Member Maloney, and distinguished Members of the Subcommittee, I am Jim Freis, Director of the Financial Crimes Enforcement Network (FinCEN), and I appreciate the opportunity to appear before you today to discuss FinCEN's ongoing role in the Administration's efforts to establish a meaningful regulatory framework for new payment methods entering into the financial system. We appreciate the Subcommittee's interest in this important issue, and your continued support of our efforts to help prevent criminal abuse of the financial system and to mitigate the risk that criminals could exploit potential gaps in our regulatory structure as technological advances create new and innovative ways to move money.

FinCEN's mission is to enhance the integrity of financial systems by facilitating the detection and deterrence of financial crime. FinCEN works to achieve its mission through a broad range of interrelated strategies, including:

- Implementing, administering, and enforcing the Bank Secrecy Act (BSA) - the United States' primary anti-money laundering (AML)/counter-terrorist financing (CFT) regulatory regime;
- Supporting law enforcement, intelligence, and regulatory agencies through the sharing and analysis of financial intelligence; and,
- Building global cooperation and technical expertise among financial intelligence units throughout the world.

To accomplish these activities, FinCEN employs a team comprised of approximately 300 dedicated employees, including analysts, regulatory specialists, international specialists, technology experts, lawyers, administrators, managers, and Federal agents.

FinCEN's main goal in administering the BSA is to increase the transparency of the U.S. financial system so that money laundering, terrorist financing, and other economic crime can be detected, investigated, prosecuted, and ultimately prevented. Our ability to work closely with our regulatory, law enforcement, international, and industry partners promotes consistency across our regulatory regime and better protects the U.S. financial system.

There are three generally understood stages of money laundering – placement, layering, and integration – and FinCEN's rules for prepaid access, including mobile payments, are specifically designed to make this more difficult to occur in significant amounts without leaving a trail and with obligations on the industry to alert FinCEN of red flags. The customer identification process addresses integration, and we see reflected in the AML policies of many financial service providers controls to limit the dollar value available to single individuals both through thresholds and tracking to prevent a single individual from purchasing multiple access devices to

avoid the thresholds. Part of the monitoring process that is a component of an AML program would generally include classic money laundering indicators, and this is where a knowledgeable institution will often be able to distinguish between legitimate and illicit activity, which may trigger a suspicious activity report that the government uses to determine if this is indeed an aspect of criminal activity. A careful monitoring of the links between emerging payment technologies and traditional financial services helps in mitigating the risks of all three stages of money laundering.

At the outset, I would like to confirm our understanding of the differences between mobile banking and mobile payments. While mobile banking involves communication and direction from an account holder about their account at a depository institution, mobile payments essentially involve the direction of funds outside of a bank account to effect payments or other transfers. In its seminal study about mobile phone-based financial services,[1] the World Bank categorized mobile banking and mobile payment activity into four different types:

- Mobile phone-based access to information about balances and transactions conducted through a financial institution (mobile banking).
- Mobile phone-based access to an account established at a financial institution, to order such financial institution to conduct payments out of the established account (mobile banking).

[1] Integrity in Mobile Phone Financial Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing, The International Bank for Reconstruction and Development/The World Bank, 2008. http://www.wds.worldbank.org/external/default/WDSContentServer/IW3P/IB/2008/09/17/000333038_20080917011913/Rendered/PDF/443840REVISED01ne01010200801PUBLIC1.pdf.

- Mobile phone-based access to an account established at a telecommunications provider, which might or might not be a financial institution, and where the account may be funded in advance or in arrears (mobile payments); note that this model exists in some foreign jurisdictions, but presently does not appear to be gaining popularity in the United States.
- Mobile phone-based access to an account established at a telecommunications provider, where prepaid phone minutes themselves are used as a virtual currency (mobile payments).

Let me emphasize that each of the foregoing are subject to relevant FinCEN regulations for AML/CFT purposes, either as part of the requirements on banks applying to all of their products and services, or as part of the requirements on money transmitters, a subset of regulated "money services businesses." While payment systems are evolving rapidly, often making leaps in functionality and connectivity within a matter of months, the aforementioned World Bank study still provides a valuable map to track the regulatory approach to the different roles mobile technology may play in the context of financial transactions. Although the World Bank study focuses on mobile financial services specifically, the same characterizations outlined above can apply with respect to mobile phones, key fobs and specialized readers, computer login over the internet, or any other means used to establish electronic communication with respect to, or to gain access to, funds. FinCEN's regulations take a comprehensive approach in this area, focusing more on the activity at issue as opposed to the particular electronic communication vehicle. For example, with respect to the first two characterizations listed above, FinCEN has already made clear that services that only provide connectivity between a customer and the financial institution where the customer account is maintained are not separately covered by

FinCEN's regulation. Responsibility under the regulations implementing the Bank Secrecy Act falls squarely on the financial institution where the account or analogous customer relationship is located, be it a bank, a securities company, or a money services business.[2]

With respect to the second two characterizations, FinCEN's regulations also have made it clear that the acceptance and transmission of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another person or location, by any means, constitutes money transmission, and that any person wherever located doing business wholly or in substantial part within the United States engaging in money transmission, regardless of any other business lines the person is engaged in – such as the provision of telecommunication services – would likely be a money services business under FinCEN's regulations, and as such must register and comply with all the reporting, recordkeeping, and monitoring requirements applicable to a money transmitter.[3] Note that there is no de minimis exception for money transmitters to be subject to regulation as a money services business; this is sometimes referred to as a "zero dollar threshold." Finally, FinCEN also has determined the obligations under its regulations that would apply to any person who sets up an arrangement involving one or more parties under a program to provide access to funds that have been paid in advance and can be retrieved or transferred through an electronic device, and to any person that participates in such prepaid access program as a Provider of prepaid access.

As FinCEN's more extensive regulation of prepaid access providers and sellers is relatively recent, and some of its details and characteristics might not be familiar to all members of this

[2] FIN-2009-R001 – "FinCEN Issues Ruling (FIN-2009-R001) on Whether Certain Operations of a Service Provider to Prepaid Stored Value Program Participants is a Money Services Business" - 03/10/2009.
[3] *See* 31 CFR 1010.100(ff).

Committee yet, let me concentrate on a brief description of the evolution of prepaid access regulation, from its inception as stored value, and its application to certain business models that might be employed by mobile payment providers.

**Mitigating Money Laundering Vulnerabilities in Prepaid Access Devices**

In dealing with prepaid access, just as is the case in approaching any financial sector, one of our biggest challenges as a regulator of financial institutions is striking the right balance between the costs and benefits of regulation. Recognizing the emergence of sophisticated payment methods and the potential for abuse by criminal actors, several years ago FinCEN began working with our law enforcement and regulatory counterparts and the industries we regulate to study the stored value/prepaid card industry in the context of expanding AML obligations to emerging payment systems. When FinCEN issued its first rule regarding money services businesses (MSBs) over a decade ago, it limited certain requirements for the prepaid or stored value arena based on varied and emerging business models, the desire to avoid inhibiting development, and other unintended consequences with respect to an industry, which at the time was in its infancy. Over time, however, it was clear that more comprehensive regulations were needed. Recognizing the importance and value of bringing a cross-section of experts together to study this issue, in May 2008, FinCEN formally established a subcommittee to focus on stored value issues within the Bank Secrecy Act Advisory Group (BSAAG). The BSAAG is a Congressionally-chartered forum[1] that brings together representatives from the financial services industry, law enforcement, and the regulatory community to advise FinCEN in its regulatory functions. The now renamed prepaid access subcommittee provides a comprehensive panel of experts available to consult on these issues and from whom a body of empirical information is gathered and exchanged.

Prepaid access is attractive to customers who do not have similar easy-to-obtain options for non-cash payments or the ability to conduct transactions remotely. But the ease with which prepaid access can be obtained and used, combined with the potential for the relatively high velocity of money moving through accounts involving prepaid access, and the potential, in some cases, for anonymity could make it particularly attractive to illicit actors. Criminals value the ability to receive and distribute a significant amount of funds without being subject to many of the reporting or recordkeeping requirements that would apply to similar transactions using cash or involving an ordinary demand deposit account at a bank.

FinCEN began to take formal steps to address this industry sector – including seeking public comment on how stored value should be defined and related issues in the proposed rule, Amendment to the Bank Secrecy Act Regulations – Definitions and Other Regulations Relating to Money Services Businesses.[ii] After we had begun efforts to revise our regulations, on May 22, 2009, President Obama signed the Credit Card Accountability, Responsibility, and Disclosure (CARD) Act of 2009.[iii] Section 503 of the CARD Act directed FinCEN, as administrator of the BSA, to issue regulations regarding the sale, issuance, redemption, or international transport of stored value, including prepaid devices such as plastic cards, mobile phones, electronic serial numbers, key fobs and/or other mechanisms that provide access to funds that have been paid for in advance and are retrievable and transferable. Although FinCEN had taken steps toward more comprehensive regulations for the prepaid/stored value sector before the CARD Act became law, the statute accelerated our timeframe.

After extensive study, consultation with the Department of Homeland Security and various other law enforcement and regulatory agencies, and a solicitation of public comments through a formal

notice of proposed rulemaking, on July 29, 2011, FinCEN published a final regulation amending Bank Secrecy Act Regulations – Definitions and Other Regulations Relating to Prepaid Access,[iv] amending the money services businesses (MSB) rules and establishing more comprehensive regulations for prepaid access.

The final regulation's most important provisions are as follows:

- It renames "stored value" as "prepaid access," without narrowing or broadening the meaning of the term, but to more aptly describe the underlying activity.
- It adopts a targeted approach to regulating sellers of prepaid access products, focusing on the sale of prepaid access products whose inherent features or high dollar amounts pose heightened money laundering risks.
- It excludes from the rule prepaid access products of $1,000 or less and payroll products, if they cannot be used internationally, do not permit transfers among users, and cannot be reloaded from a non-depository source.
- It excludes closed loop prepaid access products that provide access to less than $2,000 on any day.
- It excludes government funded and pre-tax flexible spending for health and dependent care funded prepaid access programs.

The final rule addresses regulatory gaps that have resulted from the proliferation of prepaid access innovations over the last 12 years and their increasing use as an accepted payment method. FinCEN's prepaid access regulation also provides a balance to empower law enforcement with the information needed to attack money laundering, terrorist financing, and

other illicit transactions through the financial system while preserving innovation in this rapidly growing area of consumer payments and the many legitimate uses and societal benefits offered by prepaid access. Moreover, while prepaid access is most often associated with a card, the new regulation was designed to be technology neutral to allow it to be adaptable to a range of products, such as a plastic card, an internet system, a mobile phone network, and other forms of developing technology that enable the ability to introduce and realize monetary value.

Under FinCEN's regulation, non-bank providers of prepaid access are now subject to comprehensive requirements similar to depository institutions. The final regulation reflects FinCEN's attempts to achieve the right balance. FinCEN believes that certain prepaid programs operate in such a way as to reduce potential money laundering threats and are therefore generally not subject to the provisions of the regulation. Such products include payroll cards, government benefits cards, health care access cards, closed loop cards, and low dollar products with strong safeguards in place.

Other risk variables -- such as whether a product is reloadable, can be transferred to other consumers, or can be used to transfer funds outside the country – were all things that we identified through our extensive regulatory, law enforcement, and industry consultations. When developing the regulation, we asked the general public to help validate whether we found the right balance so that higher-risk persons and products are appropriately regulated while lower-risk products are not subject to undue regulatory obligations or constraints. For the sake of clarity, let me emphasize that a payment system allowing the transfer of funds from one mobile phone to another, such as by reference to a phone number, is subject to FinCEN's regulations for prepaid access

Separately, FinCEN is nearing finalization of a rule that would include the reporting of tangible prepaid access devices as part of the current requirement to report more than $10,000 in currency or monetary instruments when crossing the border.[4]

**Subsequent Outreach to the Prepaid Access Industry**

Shortly after the publication of the final prepaid access regulation and as part of FinCEN's ongoing commitment to engage in dialogue with the financial industry and continually learn more about the industries that we regulate, FinCEN announced in October 2011 its interest in holding town hall meetings in its Vienna, Virginia offices with representatives from the prepaid access industry. The town halls were designed to elicit feedback on the implications of recent regulatory responsibilities imposed on this industry, and to receive industry's input on where additional guidance would be helpful to facilitate compliance. This outreach was intended as a part of FinCEN's overall efforts to increase knowledge and understanding of the regulated industry and how its members are affected by regulations, and thereby help FinCEN most efficiently and effectively work with regulated entities to further the common goals of the detection and deterrence of financial crime.

In response to the open invitation, FinCEN was contacted by 49 entities expressing an interest in attending the town hall meetings. Based on the information provided by the entities, FinCEN selected a representative cross-section of 16 entities that described themselves as engaging in activities that would likely fall under FinCEN's new regulatory definition of provider of prepaid access, or that acted as service providers to banks or potential providers of prepaid access. Town halls were held on November 17 and 29, 2011. FinCEN has released a number of pieces of

[4] Bank Secrecy Act Regulations: Definition of Monetary Instrument, 76 FR 64049 (Oct. 17, 2011).

guidance with respect to the prepaid access regulations and anticipates that additional guidance will be forthcoming related to some of the issues raised by the industry attendees during those town halls and through other ongoing requests for clarification and guidance on the new regulations.

**FinCEN's Efforts with Respect to Mobile Payments**

In the mobile payments universe, as noted in the World Bank study, a mobile phone can typically be used as an access device or method of communication and instruction to access accounts, initiate payment instructions, and/or notify the recipient by way of text messaging of the receipt of funds into their account. In a similar manner, so-called "mobile wallets" can be established, typically in conjunction with subscriptions to telecommunications companies, which can serve as mobile payment initiation or receipt points for customers. For some of the larger MSBs that have recently entered into the mobile payments space – such as Western Union, MoneyGram, and PayPal – the operational aspects of the actual money transfer and payment transaction segment remains similar to traditional methods of funds transfer processes facilitated by the companies, where the basic transaction flows and related recordkeeping obligations remains relatively consistent but with the mobile aspect (recipient's mobile phone number) added to it.

As part of our ongoing support to law enforcement, FinCEN provides reference manuals to help better understand the workings of various payment mechanisms and to provide steps to utilize this understanding in specific criminal investigations, including ways to subpoena records and interpret them. One recent such manual focused on mobile payments, and we have lent FinCEN's expertise in emerging payment technologies, including mobile payments, in a range of

law enforcement sensitive notices to our customers in addition to individual case support. In preparing the manual and in subsequent law enforcement outreach we have seen an interesting trend in the mobile payments industry where different telecommunication systems and/or financial mechanisms may merge and become interwoven in the same overall mobile payments transaction. For example, a customer may choose to initiate a remittance through a traditional, brick-and-mortar MSB agent location with the transaction then being processed through that MSB's centralized internal system, and the payment of funds then going to a recipient's mobile wallet account. Upon completion of the transaction, the recipient typically receives a text message notification on their mobile phone that indicates the funds have been credited to their mobile wallet account. The recipient also then may be able to withdraw the funds at an ATM via a debit card. This transactional overlap often provides multiple informational choke points that potentially lead to each other, which may, in turn, actually pose a benefit to law enforcement in their efforts to follow the money trails and identify other accounts and transactions associated with a given subject(s). Borrowing from procedures provided to FinCEN by one of the nation's largest providers of mobile payment services, consider the following scenario as an illustration of how a typical transaction from the United States to the Philippines might work:

- A customer goes to a domestic MSB agent facility and completes a standard money remittance form, including the recipient's mobile number;
- The funds are transferred through the MSB's internal processing system to a recipient's "SMART Money" account that is affiliated with a participating communications company and the account is maintained at a financial institution in the Philippines.
- The recipient receives a text message notifying them that the funds are now available, at which point the recipient can then either use their mobile phone to transfer funds to

another SMART Money account, reload airtime, pay bills with participating merchants, or retrieve the funds directly from an ATM through the use of a SMART Money card (similar to a debit card).

As discussed previously, FinCEN's prepaid access regulation was specifically designed to be flexible and to accommodate new technologies as they emerge, but also to capture innovative payment methods currently used by U.S. institutions, including aspects of the scenario described above. In addition, FinCEN's money transmitter regulations also may serve as a basis for regulating aspects of such activity. Consistent with past practice, FinCEN will interpret its regulations as they apply to various business models and provide guidance as necessary to industry with respect to the application of FinCEN's requirements.

**Conclusion**

In the area of new payment methods, the Administration has made appropriate oversight of prepaid access products a priority, and as a result the Treasury Department's efforts in this regard have increased significantly over recent years through targeted regulatory measures, outreach to regulatory and law enforcement counterparts and our partners in the private sector. In addition, FinCEN's regulations in the MSB space, whether in the context of prepaid access or money transmission, can apply to select actors in the mobile payments space depending on the variety of business models that develop. We are very encouraged by the progress we have made thus far, and we are dedicated to continuing to build on these accomplishments as we chart a course for the future that encourages legitimate consumer and commercial activity to flourish, but also helps financial services providers to focus on serving their customers, not criminals. Thank you

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

[i] http://www.ffiec.gov/bsa_aml_infobase/documents/regulations/Annunzio_Wylie.pdf
[ii] 74 FR 22129 (May 12, 2009)
[iii] http://www.gpo.gov/fdsys/pkg/PLAW-111publ24/pdf/PLAW-111publ24.pdf
[iv] http://www.gpo.gov/fdsys/pkg/FR-2011-07-29/pdf/2011-19116.pdf

For release on delivery
9:30 a.m. EDT
June 29, 2012

Statement by

Stephanie Martin

Associate General Counsel

Board of Governors of the Federal Reserve System

before the

Committee on Financial Services

Subcommittee on Financial Institutions and Consumer Credit

U.S. House of Representatives

Washington, D.C.

June 29, 2012

Chairman Capito, Ranking Member Maloney, and members of the Subcommittee, thank you for inviting me to appear before you today to talk about the regulation of mobile payments.

The evolution of technologies that enable consumers to conduct financial transactions using mobile devices has the potential to affect their financial lives in important and new ways. In discussing "mobile payments," I am referring to 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 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. These 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 there are important issues to consider, such as the reliability and security of these technologies.

With any type of payment system, including mobile payment systems, regulators have two key concerns: (1) whether consumers are protected if something goes wrong, such as an unauthorized transaction; and (2) whether the system provides appropriate security and confidentiality for the transmission and storage of payment instructions and the personal financial information of consumers.

A legal framework exists to address the payment activities of insured depository institutions--collectively, "banks." This framework includes consumer protection statutes, such as 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. Even so, many of our payments laws were initially drafted long before mobile payments (or the devices that facilitate them) were even envisioned. Therefore, those laws may not be well-tailored to address the full range of mobile payment services in the marketplace.

**The Evolution of Payments**

The U.S. payments landscape has changed dramatically in recent decades and continues to evolve rapidly. Electronic payments made through payment card networks and the automated clearinghouse system have become increasingly prevalent, and now represent about four out of every five noncash payments in this country.[1] 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 payments encompasses a combination of continued advances in hardware, software, and payment systems. These advances include contactless payments, online banking, mobile phones (particularly smart phones) and other remote devices, applications, and the convergence of Internet or e-commerce and mobile commerce.

At its core, however, a mobile payment, like any other type of payment, results in money moving between bank accounts--for example, from a consumer's checking account at the consumer's bank to the merchant's checking account at the merchant's bank. This is true even if the payment initially is charged to a consumer's bill for services or to a prepaid balance held by a nonbank. For example, in the case of a mobile payment charged to a phone bill, ultimately, the

---

[1] See the 2010 Federal Reserve Payments Study, www.frbservices.org/files/communications/pdf/press/2010_payments_study.pdf.

consumer pays the bill with funds from an account at a bank. In the "back end" bank-to-bank settlement of these payments, the funds will typically travel on existing payment "rails," such as the automated clearinghouse system or a card network. The settlements between bank accounts over these existing systems are subject to the statutes, rules, or procedures that are already in place.

There are, though, new and evolving aspects of mobile payments--typically related to the consumer interface and nontraditional payment or settlement arrangements--which can involve new types of intermediaries or service providers. A new interface is not a new phenomenon. The evolution of consumer payments has gone from paper checks to debit and credit cards to home banking through personal computers and is now moving to smart phones and other remote devices, which have some of the processing and communications characteristics of home computers. In the case of bank-offered payment products, a new communication channel to an existing payment mechanism, such as a smart phone connection to the debit card or credit card system, generally does not result in changes to the basic rights afforded to consumers under those systems or to a bank's responsibility to ensure the security of that communication channel.

However, consumers may make payments in new ways using the services of entities that have not traditionally been in the payments business. For example, a consumer may settle a mobile payment transaction via a bill from a telephone company. Making payments through nontraditional arrangements may change the legal protections related to the purchase, depending on the details of the arrangement and the applicable federal or state statutes and rules.

**Regulation of Mobile Payment Services Offered by Banks**

As I stated, a legal framework to address the activities of banks already is in place, and to the extent that existing laws and rules apply, federal bank regulators have the tools to ensure that banks offer mobile payment services in compliance with the consumer protection provisions of those laws and rules. For example, electronic debits or credits to certain consumer asset accounts would generally be covered by the error-resolution, disclosure, and other provisions of the EFTA. The application of this act and most other federal consumer laws to bank or nonbank mobile payment transactions, including the extent to which transactions involving prepaid balances are covered, is subject to the rulemaking and interpretive authority of the Consumer Financial Protection Bureau (CFPB).

When reviewing new payment interfaces that banks offer to their customers, the banking agencies look at the security and confidentiality protections that the bank has instituted. For example, the Federal Financial Institutions Examination Council Information Technology Handbooks provide guidance to examiners and financial institutions on identifying and controlling the information-security risks associated with electronic banking activities, including banking through mobile phones. Under section 501(b) of the Gramm-Leach-Bliley Act (GLBA), banks are required to implement programs that ensure the security and confidentiality of customer information, protect against unanticipated threats or hazards to the security or integrity of that information, protect against unauthorized access to or use of information that could result in substantial harm or inconvenience to any customer, and ensure the proper disposal of customer information. Banks are also subject to the so-called "red flags" rules that require financial institutions and creditors to implement programs designed to detect, prevent, and

mitigate identity theft, as well as a variety of anti-money-laundering and other rules under the Bank Secrecy Act.

**Regulation of Mobile Payment Services Offered by Nonbanks**

Many of the questions that have arisen with respect to mobile payments, however, relate to the involvement of nonbanks as intermediaries or service providers. The applicability of existing laws to nonbanks that are providing mobile payment services often depends on the nonbank's role in the transaction. For example, a bank might use a payments processor to offer its customers a means to initiate payments to third parties from mobile phones. In that case, the bank would continue to be responsible for ensuring that its agent complies with the laws and rules that are applicable to the bank. In other cases, however, a nonbank can have a more independent role, such as a manager of a prepaid value program, a money transmitter, or a telephone company that bills customers for payment transactions. In these cases, it is necessary to examine the specific provisions of law to determine their applicability to the nonbank's particular role in the transaction.

As I mentioned earlier, the applicability of many federal consumer laws, such as the EFTA, to mobile payment services is subject to the rulemaking and interpretation of the CFPB. Other laws also may apply, depending on the specific facts and circumstances of the arrangement. For example, the security guidelines mandated by section 501(b) of the GLBA and the "red flags" rules apply to certain nonbank entities that engage in financial activities as well as to banks, and therefore could be applicable to a nonbank's mobile payment interface with consumers. The Federal Trade Commission administers these requirements to the extent they apply to nonbanking firms. Further, the Treasury Department's Financial Crimes Enforcement

Network (commonly known as FinCEN) applies know-your-customer and anti-money-laundering rules to providers and sellers of certain types of prepaid access, including prepaid cards.[2]

A nonbank service provider also may be subject to state money transmitter laws. Although these laws are not uniform among the states, many of them include registration and bonding requirements and investment restrictions.

For international payments, both bank and nonbank service providers may also be subject to the remittance provisions in the EFTA, as implemented by the CFPB.

**Conclusion**

In conclusion, it is difficult to make broad generalizations about the applicability of existing statutes and rules to mobile payments. This is due to the different types of service providers (bank and nonbank), the wide variety of payment arrangements that are in place and under development, and the potential applicability of both banking and nonbanking laws to any given arrangement. Given recent technological developments in mobile payments, further analysis of existing laws may be needed to ensure that consumers are adequately protected. At the same time, 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.

Thank you again for inviting me to appear today. I am happy to answer any of your questions.

---

[2] 31 CFR 1010.100(ff).


**Statement for the Record**
**House Financial Services Committee**
**Subcommittee on Financial Institutions and Consumer Credit**
**"The Future of Money,...#157"**

The Clearing House Association L.L.C. ("The Clearing House")[1] appreciates the opportunity to submit this statement for the record in connection with the June 29, 2012, hearing before the House Committee on Financial Services Subcommittee on Financial Institutions and Consumer Credit.

Mobile phones and other devices are increasingly being used to initiate payment transactions in the United States and are expected to begin to displace magnetic-stripe payment cards for consumer payments. The adoption of mobile payments technology holds the potential to vastly expand financial inclusion and facilitate growth in commerce. At the same time, the rapid expansion of mobile payments has introduced new payment service providers and mechanisms into the payment system, which bring with them the potential to create new risks. Payment integrity, security, and other consumer protections, once the domain of highly regulated, supervised, and examined depository institutions, are now influenced by mobile phone manufacturers, mobile phone network operators, application developers, and providers of Internet services, including social media. Although some of these service providers and mechanisms are subject to existing consumer protections under federal laws and regulations, others are not. Even in cases where existing federal payments rules may apply, these new entrants raise new issues and present new challenges for regulators and consumers.

We believe that:

- the varying regulatory structures applicable to mobile payment providers yield uncertain consumer protections and uneven oversight of the safety and soundness of various payment systems;
- the complex and fragmented mobile payments ecosystem has the potential to create a confusing consumer experience, increase the risk of fraud, and create new risks to the protection and management of customer bank data; and
- the evolving mobile payments environment presents significant issues that will need to be addressed to ensure that law enforcement has the tools it needs to successfully monitor, track, and prevent money laundering and terrorist financing.

[1] Established in 1853, The Clearing House is the nation's oldest banking association and payments company. It is owned by the world's largest commercial banks, which collectively employ 1.4 million people in the United States and hold more than half of all U.S. deposits. The Association is a nonpartisan advocacy organization representing—through regulatory comment letters, amicus briefs, and white papers—the interests of its owner banks on a variety of systemically important banking issues. Its affiliate, The Clearing House Payments Company L.L.C., provides payment, clearing, and settlement services to its member banks and other financial institutions, clearing almost $2 trillion daily and representing nearly half of the funds transfer, automated clearinghouse, and check image payments made in the United States. For additional information, see The Clearing House's Web page at www.theclearinghouse.org.

**I. The varying regulatory structures applicable to mobile payment providers yield uncertain consumer protections and uneven oversight of the safety and soundness of various payment systems.**

Mobile payments commonly refer to payments initiated through a mobile phone or a mobile Internet communication device such as a smartphone or a tablet. The pervasive access to mobile phones throughout the population and the growing ubiquity of smartphones holds significant promise for the rapid growth of mobile commerce in the United States and the provision of payment methods to previously underbanked populations.[2] At the same time, divergent mobile technology models and the diversity of entrants into the mobile space also present significant regulatory challenges.

Mobile payments can generally be divided into two categories: proximity payments, where technology embedded in or displayed on the payor's mobile device interfaces with the payee's point-of-sale equipment to initiate payment (e.g., near field communication, barcode or QR code), and remote payments, where the payor uses the mobile device to initiate payment to the payee without regard to proximity to the payee or point-of-sale equipment. Mobile phones greatly facilitate the communication aspects of payments and open the door to many new payment methods and channels.

This vast potential for communication can be readily coupled with an agreement with the consumer using the mobile phone that binds the consumer and obligates the consumer on the payment. This agreement can be with the mobile network or with a third party providing a service that can be accessed through the mobile phone.

The broad communication ability of mobile phones and a ready means of binding the consumer to the payment obligation make the means of settling the payment the primary constraint on mobile payments. Viewed from a settlement perspective, mobile payments diverge widely, falling into three general models—bank payments, money transmitter payments, and mobile network payments.[3]

Mobile phones can serve as devices for accessing traditional bank payments including credit card, debit card, and automated clearinghouse payments. In these cases the phone merely substitutes for other access devices, such as the familiar plastic credit or debit card, and payments are processed through interbank arrangements subject to existing legal requirements, including well-established federal consumer protection laws.[4] Mobile payment services offered by banks must also comply with the significant regulatory guidance applicable to banks and are conducted under the extensive standards

---

[2] Mobile phone use is high among groups that are prone to be unbanked or underbanked according to a recent study released by the Board of Governors of the Federal Reserve System (Consumers and Mobile Financial Services, March 2012).

[3] It should be noted that these three categories are somewhat simplified. The mobile ecosystem is emerging in complex ways and there can be many variations on the basic models discussed here. It should also be noted that the word "bank" is being used in a broad sense to include banks, credit unions, and other depository financial institutions.

[4] Applicable law includes the Truth in Lending Act ("TILA") for credit card payments and the Electronic Fund Transfer Act ("EFTA") for payments initiated out of bank deposit accounts held in the name of a consumer making the payment. These laws provide important consumer rights including the right to receive monthly statements describing transactions, the right to have billing errors addressed, and, subject to certain conditions, the right to have unauthorized transactions reversed. In the case of credit card transactions, these rights also include the ability to assert claims and defenses that the holder has against the merchant, subject to specified conditions.

and examination procedures adopted by bank supervisors and, more recently, the Consumer Financial Protection Bureau ("CFPB").[5]

Mobile phones can also access the services of nonbank money transmitters. In doing so, mobile phones, as well as other electronic communications, have the potential to greatly increase the use of these services by providing more convenient access and facilitating the delivery of payments to payees, who may be notified of the payment through their own electronic or mobile devices. Money transmitter payments are not subject to the full panoply of bank regulation and supervision. While certain aspects of their business have been subject to federal oversight, such as federal anti-money laundering requirements and, depending upon their business model, some aspects of their business may be subject to federal consumer protection laws such as the Electronic Fund Transfer Act, the transmitters themselves, to date, have only been subject to supervision and oversight under state laws.[6] These state laws vary and may not cover all mobile applications or service providers that provide access to money transmitter payments, because their activities are limited to the communication aspects of the payment and do not include a settlement function.

Finally, payments initiated through mobile phones can be settled through the mobile phone network itself either by billing the transaction to the mobile phone holder's account with the network or by charging the payments to a prepaid card or phone account. Mobile phone networks are under the general oversight of the Federal Communications Commission and operate under a regulatory and supervisory regime that vastly differs from the regulatory and supervisory regime that applies to banking organizations or even the more limited state law regime that applies to money transmitters.[7] Although in some cases federal consumer protection laws that also apply to bank payment services may apply, the bank supervisory regime does not, making enforcement of these laws, as well as the security and integrity of the payment process, less certain.[8]

Because the multitude of nonbank players entering the mobile payments ecosystem are generally not subject to the same functional regulation that applies to depository institutions, they are considered "shadow payments providers." The patchwork of regulatory and supervisory regimes applicable to shadow payment providers leaves consumers with varied and often uncertain protections and a supervisory and examination structure that unevenly regulates the soundness and integrity of providers in the mobile payments space. For example, shadow payment providers are in some

---

[5] By federal law, with some exceptions, banks receive at least one full-scope, on site examination at least once during each year (every 18 months under certain circumstances). The examination process is supported by supervisory guidance that addresses both compliance with laws applicable to mobile payments services and the management, technology, and operations infrastructure necessary to support mobile payments.

[6] EFTA and its implementing regulatory protections may apply if the money transmitter offers the customer an account in which to hold funds.

[7] For example, while billing error rights are a focus of the consumer protections provided under TILA for credit cards and EFTA for electronic payments out of bank deposit or other consumer accounts, a consumer's recourse for a billing dispute with a mobile phone carrier is to complain to the Federal Communications Commission, which will endeavor to resolve the issue.

[8] As in the case of money transmitter payments, the supervisory guidance developed through decades of experience that strengthens the platform for payments though the banking system is absent, as is the experienced and skilled examination conducted by federal bank examiners.

circumstances subject to more limited regulatory requirements than banks in key areas such as "know your customer" and anti-money laundering.

In general, the entrance of less-supervised providers is likely to result in a reduction in the reliability and integrity of payments. The extent to which this reduction results in significant harm to consumers will depend, in part, on the extent to which mobile payments are covered by existing regulatory regimes such as the Truth in Lending Act and the Electronic Fund Transfer Act. However, coverage by these laws alone will not be sufficient to ensure comparable consumer protections. Such coverage would need to be supplemented by a robust and rigorous regime of supervision and enforcement.

**II. The complex and fragmented mobile payments ecosystem has the potential to create a confusing consumer experience, increase the risk of fraud, and create new risks to the protection and management of customer bank data.**

Historically, the customer bank data (personal account information) necessary to authorize payment transactions has been issued by banks to consumers in finite, recognizable forms that consumers readily understood required protection. Checkbooks were guarded in safe places, checks were manufactured with features to prevent counterfeiting, and authorized signatures were required for negotiation. Credit and debit cards were issued in plastic format, were kept in wallets or purses, and, as time went by, were imbued with additional security features, such as picture IDs or specially encoded information. The issuer of the customer bank data was listed on the check or card and was readily understood by the consumer to be the party the consumer needed to contact should the payment vehicle containing the customer's bank data be lost, stolen, or otherwise compromised. When notified, banks easily cancelled and reissued cards or checks and changed account numbers.

Over time, banks also developed sophisticated fraud detection systems with artificial intelligence capable of using customer profiles and historical transactional information to evaluate in real time the likelihood that a given transaction was fraudulent, thereby limiting the risk of unauthorized charges to the consumer's account. The law developed within this historical context to limit, within certain constraints, a consumer's liability for fraudulent transactions.

However, as the mobile payments ecosystem is evolving, consumers are being confronted with an ever-dizzying array of business and technology models including some that rely on customer transactional and geolocation data to engage in targeted advertising. The result is a plethora of parties and payment devices that may store customer bank data. As a result, without careful product structuring by a regulated bank, consumers may be left without a clear understanding of what to do when an unauthorized charge occurs or a payment device is lost or stolen. For example, a consumer may be issued a credit card by a bank which the consumer then "stores" in the consumer's mobile phone through the use of an application provided by an application developer. Does the consumer now realize that his or her phone has now become the equivalent of a physical wallet and needs to be protected with the same degree of security and vigilance? If the consumer's phone is stolen, or an unauthorized transaction occurs, does the consumer call the mobile phone provider, the app developer, or the consumer's bank? Banks are well positioned, based on their extensive experience in payments, to develop mobile payments products that provide customers the level of security and customer service they expect based on their experience with traditional payments products such as checks and credit cards.

The emerging number of mobile wallets (including "cloud-based wallets" where the payment information is not stored on the device or provisioned securely by a bank issuer) and other devices within which customer bank data can be stored makes it difficult for consumers and issuers to seamlessly and reliably track and update customer bank data when needed. The growing complexity of this system is not only likely to increase security risks, but may result in customer confusion and frustration, lost transactions for merchants, and support system nightmares for issuers.

In addition, shadow payments providers often disintermediate the messaging of traditionally regulated systems, inserting themselves into the transaction as the merchant of record. Thus, the merchant of record that may appear on a consumer's bank statement may be the shadow payments provider rather than the actual entity from whom the consumer actually purchased goods or services. This is likely to cause consumer confusion as to the true nature of the charge, whether the charge is fraudulent or erroneous, and the proper means through which a potential dispute should be resolved. Further, because the merchant of record is not the merchant in fact, the sophisticated fraud detection systems banks have built to monitor transactions in real time may be impaired in their ability to receive data (the identity of the merchant or the real nature of the goods or services purchased) useful in fraud prevention.

Finally, under the current regulatory scheme, banks are usually required to absorb fraud liability and always absorb the cost of recredentialing regardless of whether they had any connection with the underlying breach that compromised the data. Because the liability and costs of fraud are not always properly aligned with the responsibility, other players in the mobile ecosystem may have less of an incentive to develop stringent security safeguards and standards to reduce incidents of fraud, particularly in the absence of an effective regulatory regime. Ultimately, this would result in higher costs to consumers and merchants as the costs of fraud liability protection increase.

**III. The evolving mobile payments environment presents significant issues that will need to be addressed to ensure that law enforcement has the tools it needs to successfully monitor, track, and prevent money laundering and terrorist financing.**

The Bank Secrecy Act ("BSA") and FinCEN's anti-money laundering ("AML") regulations serve the important public-policy goal of discouraging money laundering and terrorist financing by enlisting financial institutions in this effort. The financial institutions covered under these requirements include depository institutions, money services businesses, credit-card system operators, and insurance companies along with businesses such as casinos and dealers in precious jewels.

The regulations impose four basic types of requirements on these financial institutions: filing reports of certain transactions, record-retention requirements, customer due diligence responsibilities, and active monitoring for suspicious activities. The reports (including Currency Transaction Reports and Suspicious Activity Reports) provide FinCEN and other law-enforcement agencies with information on transactions, currency flows, and suspicious activity so they can study trends and deploy their resources effectively. The record-retention requirements provide law enforcement the opportunity to get a complete picture of a suspect's financial transactions and relationships including any payees, sources of funds, and other transactions.

As the mobile payments environment evolves, significant issues will need to be addressed to ensure that law enforcement has the tools it needs to monitor, track, and prevent money laundering and

terrorist financing. The disintermediation effect that shadow payment providers can have in the mobile space can add a significant layer of complexity to an effective AML regime.

If the shadow payment provider appears as the merchant of record, either as the payee or the source of funds for a consumer's bank transactions with another consumer or merchant, bank records will not disclose to law enforcement the true payee or source of funds for the real transaction. By disintermediating banks from the actual beneficial parties of the end-to-end payment transaction, banks have a less-than-comprehensive picture of the customer's financial activities and the bank's ability to monitor for suspicious activity will be compromised.

While investigators could go to the shadow payment provider to discover the identities of the actual beneficial parties to the transaction, it remains uncertain whether all shadow payments providers are subject to FinCEN's record-retention requirements, potentially denying investigators the ability to compile a complete picture of a suspect's transactions. At the very least, investigators will be deprived of a clear and efficient record of the transactions through utilization of the bank's records.

* * * * *

Although mobile payments technology holds great promise for the advancement of commerce and financial inclusion, the rapid growth and fragmented ecosystem of mobile also presents serious regulatory and oversight challenges. Providers engaged in functionally similar activities will need to be regulated and supervised in functionally equivalent ways so that important consumer protections are applied evenly across provider categories and models and that safety, soundness, and security concerns are being evenly addressed and compliance examined. Industry standards will need to be developed to ensure that customer bank data is securely and appropriately protected in all transactions and that data will be capable of being appropriately tracked and easily updated. Finally, significant issues will need to be addressed to ensure that law enforcement continues to have the tools it needs to efficiently and effectively monitor, track, and prevent money laundering and terrorist financing regardless of the nature of the provider or the business model or technology employed.

If you have any questions about this statement or would like to discuss these issues further, please contact Robert C. Hunter at (336) 769-5314 or Rob.Hunter@theclearinghouse.org.

Respectfully submitted,

**The Clearing House Association L.L.C.**

/s/

Robert C. Hunter
Deputy General Counsel

**Statement for the Record**
**Of Marla Blow, Assistant Director, Card and Payment Markets**
**Consumer Financial Protection Bureau**
**Before the**
**House Financial Services Subcommittee on Financial Institutions and Consumer Credit**
**June 29, 2012**

On behalf of the Consumer Financial Protection Bureau (CFPB or Bureau), thank you for the opportunity to provide this statement for the record about mobile payments.

The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) requires the CFPB to regulate consumer financial products and services under Federal consumer financial law. Our mission is to make consumer financial markets work for consumers, honest businesses, and the economy as a whole. In carrying out this mission, the Bureau has a key role to play in the regulatory, supervisory, and oversight regimes governing mobile payments.

Many interagency partners have substantial roles in overseeing the mobile payments market as well. The Bureau is engaged in ongoing coordination with the Federal Trade Commission, the Federal Communications Commission, the Federal Deposit Insurance Corporation, the Federal Reserve Board, the Office of the Comptroller of the Currency, the Treasury Department's Financial Crimes Enforcement Network, and state banking regulators. We are committed to working closely with state and federal partners on this issue.

Innovation in mobile payments may yield numerous, significant benefits for consumers. At the same time, it may present unique challenges. We are engaging with innovators to understand how these new technologies may transform consumer finance so that we can determine how our regulatory structure intersects with these changes.

While there is significant excitement and anticipation, there has not yet been substantial adoption of mobile payments in the United States. However, the current state of the mobile phone market and the penetration rate of smartphones suggest that broad adoption could occur quickly when the right factors align. It would be premature to speculate about what form of mobile payment system, if any, may ultimately gain widespread use and acceptance. Nonetheless, the CFPB is closely monitoring new developments and changes in the marketplace and in consumer use patterns. The primary responsibility for monitoring developments in mobile payments within the Bureau is housed in the Card and Payment Markets team, part of the division of Research, Markets, and Regulations. The Card and Payment Markets team has responsibility over Credit, Debit, Prepaid, and Mobile Payment markets. We are engaged in ongoing discussions with relevant parties, as well as other state and federal agencies.

Encouraging consumer-friendly market innovations is one of the Bureau's key goals. Developments in mobile payments represent a unique opportunity for rapid innovation. Innovation can be greatly advantageous to consumers, offering new tools for people to better control their own finances and plan their own lives. The connectivity and computing power of a modern smartphone could be used to develop rich applications that provide better services at

lower costs. These same tools could be used to better serve the unbanked and underbanked populations and provide high quality financial services to all consumers.

At the same time, innovation can introduce significant risks to consumers. New technologies may be designed in ways that may not fall within existing regulatory frameworks. Existing rules may not have anticipated new developments enabled by modern technology and may prove inadequate for addressing emerging concerns. To the extent that technology companies begin to play roles traditionally performed by banking institutions, we may need to reconsider how well our existing regulations apply to a changed environment.

While innovation and the disruption it engenders may introduce risk to consumers, there may also be risks created by the very nature of mobile payments. Mobile devices often have small screens that make meaningful disclosure difficult. This is compounded by consumers having become inured to "Terms and Conditions" that are often dozens of pages long and frequently bypassed with a single click. The quality of design and user experience on modern smartphones can be truly extraordinary – but this may cause consumers to be less critical in accepting new charges or understanding new products. A mobile wallet could steer customers to suboptimal decisions due to vested interests of the mobile wallet provider or other underlying motives. The nature of mobile handsets, operating systems, and mobile networks may provide serious interoperability challenges that could restrict consumer choice.

These are very real opportunities and very real challenges. In order to best set the stage for consumer-friendly innovation, we need to examine existing regulations to determine if there are barriers to successful mobile payment systems. We also need to see if regulations should be updated to address new concerns. And we need to meet with new market entrants and make sure market participants understand their compliance obligations under federal consumer financial protection laws. These are necessarily ongoing activities that will be repeated as the industry develops and mobile payments begin to take hold.

Our intent is to be flexible and responsive to the changing marketplace. We will continue this work in conjunction with our interagency partners to make sure that all areas of the market are subject to common "rules of the road" and that consumers' rights are protected regardless of their method of payment.