AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

THE DISRUPTER SERIES: MOBILE PAYMENTS

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

DECEMBER 1, 2015

Serial No. 114–105



Printed for the use of the Committee on Energy and Commerce
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

20–159 PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing 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

COMMITTEE ON ENERGY AND COMMERCE

FRED UPTON, Michigan
Chairman

JOE BARTON, Texas
Chairman Emeritus
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOSEPH R. PITTS, Pennsylvania
GREG WALDEN, Oregon
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
Vice Chairman
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
BILLY LONG, Missouri
RENEE L. ELLMERS, North Carolina
LARRY BUCSHON, Indiana
BILL FLORES, Texas
SUSAN W. BROOKS, Indiana
MARKWAYNE MULLIN, Oklahoma
RICHARD HUDSON, North Carolina
CHRIS COLLINS, New York
KEVIN CRAMER, North Dakota

FRANK PALLONE, JR., New Jersey
Ranking Member
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
G.K. BUTTERFIELD, North Carolina
DORIS O. MATSUI, California
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
JERRY MCNERNEY, California
PETER WELCH, Vermont
BEN RAY LUJAN, New Mexico
PAUL TONKO, New York
JOHN A. YARMUTH, Kentucky
YVETTE D. CLARKE, New York
DAVID LOEBSACK, Iowa
KURT SCHRADER, Oregon
JOSEPH P. KENNEDY, III, Massachusetts
TONY CÁRDENAS, California

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

MICHAEL C. BURGESS, Texas
Chairman

LEONARD LANCE, New Jersey
Vice Chairman
MARSHA BLACKBURN, Tennessee
GREGG HARPER, Mississippi
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
GUS M. BILIRAKIS, Florida
SUSAN W. BROOKS, Indiana
MARKWAYNE MULLIN, Oklahoma
FRED UPTON, Michigan *(ex officio)*

JANICE D. SCHAKOWSKY, Illinois
Ranking Member
YVETTE D. CLARKE, New York
JOSEPH P. KENNEDY, III, Massachusetts
TONY CÁRDENAS, California
BOBBY L. RUSH, Illinois
G.K. BUTTERFIELD, North Carolina
PETER WELCH, Vermont
FRANK PALLONE, JR., New Jersey *(ex officio)*

C O N T E N T S

Page

Hon. Michael C. Burgess, a Representative in Congress from the State of Texas, opening statement 1
Prepared statement 3
Hon. Janice D. Schakowsky, a Representative in Congress from the State of Illinois, opening statement 4
Prepared statement 5
Hon. Fred Upton, a Representative in Congress from the State of Michigan, opening statement 5
Prepared statement 6
Hon. Frank Pallone, Jr., a Representative in Congress from the State of New Jersey, opening statement 7
Prepared statement 8

WITNESSES

John Muller, Vice President, Global Payments Policy, PayPal 9
Prepared statement 12
Answers to submitted questions 96
Jessica E. Deckinger, Chief Marketing Officer, Merchant Customer Exchange 20
Prepared statement 24
Answers to submitted questions 99
Sarah Jane Hughes, University Scholar and Fellow in Commercial Law, Maurer School of Law, Indiana University 33
Prepared statement 35
Answers to submitted questions 101
Sang W. Ahn, Chief Commercial Officer, U.S. Samsung Pay, Samsung Electronics America 48
Prepared statement 50
Answers to submitted questions 105

SUBMITTED MATERIAL

Statement of the Electronic Transactions Association, December 1, 2015, submitted by Mr. Lance 80
Statement of the National Association of Convenience Stores and the Society of Independent Gasoline Marketers of America, December 1, 2015, submitted by Mr. Lance 85
Statement of the National Retail Federation, December 1, 2015, submitted by Mr. Lance 91

THE DISRUPTER SERIES: MOBILE PAYMENTS

TUESDAY, DECEMBER 1, 2015

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:21 a.m., in room 2322, Rayburn House Office Building, Hon. Michael C. Burgess (chairman of the subcommittee) presiding.

Members present: Representatives Burgess, Lance, Blackburn, Harper, Guthrie, Olson, Pompeo, Kinzinger, Bilirakis, Brooks, Mullin, Upton (ex officio), Schakowsky, Clarke, Cárdenas, Welch, and Pallone (ex officio).

Staff present: Gary Andres, Staff Director; Rebecca Card, Assistant Press Secretary; James Decker, Policy Coordinator, Commerce, Manufacturing, and Trade; Andy Duberstein, Deputy Press Secretary; Graham Dufault, Counsel, Commerce, Manufacturing, and Trade; Melissa Froelich, Counsel, Commerce, Manufacturing, and Trade; Paul Nagle, Chief Counsel, Commerce, Manufacturing, and Trade; Tim Pataki, Professional Staff Member; Olivia Trusty, Professional Staff, Commerce, Manufacturing, and Trade; Dylan Vorbach, Legislative Clerk; Michelle Ash, Democratic Chief Counsel, Commerce, Manufacturing, and Trade; Christine Brennan, Democratic Press Secretary; Jeff Carroll, Democratic Staff Director; Ashley Jones, Democratic Director, Outreach and Member Services; Caroline Paris-Behr, Democratic Policy Analyst; Tim Robinson, Democratic Chief Counsel; Diana Rudd, Democratic Legal Fellow; and Ryan Skukowski, Democratic Policy Analyst.

OPENING STATEMENT OF HON. MICHAEL C. BURGESS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. BURGESS. The Subcommittee on Commerce, Manufacturing, and Trade will now come to order. The Chair will recognize himself for 5 minutes for an opening statement, and I do want to welcome everyone to our hearing this morning examining mobile payments, which are poised to upend how consumers pay for goods and services in stores, online, in apps, and at the parking meter. This hearing is the latest in our disrupter series, covering a variety of technologies that are redefining our lives and improving our or economic condition.

This past week, Black Friday, Small Business Saturday, Cyber Monday flooded all of our inboxes and took over the commercial breaks on television. As the holiday shopping season is in full

swing, this is a good time to take a look at the consumer experience with mobile payments. This morning, we will hear from our witnesses representing a variety of innovative products and services in the mobile payments arena. This hearing is an opportunity to learn about the innovations that are available to consumers today and those that will be available in the near future, but we recognize that there are exciting innovations on the horizon for payments, including mobile currencies, which will be a topic for another day.

Smartphones are increasingly an ever-present part of our lives. It is no surprise that they are also changing the way that we shop for goods and services. You can shop on your tablet in front of the television, compare prices on your phone as you browse in a store, and pay without ever pulling out your wallet. Consumers have access to more information, and more competitive options are at the tip of their fingers during the busiest shopping season of the year. There has not been this big an upheaval in how consumers pay for goods and services, from groceries to haircuts, since computers replaced the old knuckle-buster manual imprinters in the 1980s.

In 2014, 22 percent of mobile phone owners reported making a purchase with their phone; 39 percent used their phones to make a purchase in the store. When you find that perfect Christmas gift, you may be able to pay by tapping your phone at checkout or clicking the PayPal checkout button on a mobile Web site. When you want to send your friend money for the concert ticket they bought for you, all you need is their email address or their mobile phone number. These mobile payment options include protections not available with cash and are easy to use for consumers who may be more likely to have their phone in their pocket than carry the exact change with them.

Some basic questions remain top of mind for consumers when they think about mobile payments: Are they safe? Can I use my phone? This hearing is an opportunity to hear from companies implementing the cutting-edge technologies in mobile payments and how they are addressing these and other concerns raised by consumers.

Two of the top security topics that are raised by mobile payments are authentication, how the device knows you have permission to make the payment with the device, and tokenization, protecting your payment data through the payment process. We all know passwords are difficult. They are difficult to remember. They are difficult to keep straight, which is why many people—myself not included, but many people—simply use their name for their user name and 1234 as their password. Mobile devices offer some alternatives to the traditional password that add an additional layer of protection for consumers.

Authentication is the process that a system uses to verify the identity of a person that wants access to the system. The user name and password is the most typical authentication process used to log into a variety of Web sites. Mobile devices have changed. They have changed how people think about authentication. Fingerprint sensors, cameras are found in an increasing number of mobile devices; and instead of having to remember a separate password to unlock your phone or tablet, you may be able to use the fingerprint

scanner to unlock the device with just a touch. This protects the information on the phone, including access to payment options.

Another security feature that is regularly brought up in discussions about mobile payments is tokenization. We are all familiar with the tokens you get at the fair or the arcade. Tokens in a mobile payment system are similar in concept, replacing the valuable currency or payment information with a code that then becomes useless for another transaction if someone were to steal it.

As has been the case throughout history, technology has the potential to solve problems and improve our lives. Mobile payments are no exception to that trend. So I look forward this morning to hearing from our witnesses and how they are leveraging the mix of technologies to provide an easy and secure experience for United States consumers as we make our way through this shopping season.

[The prepared statement of Mr. Burgess follows:]

PREPARED STATEMENT OF HON. MICHAEL C. BURGESS

This hearing is the latest in our Disrupter Series covering a variety of technologies that are redefining our lives and improving our economic condition.

Over the last week, Black Friday, Small Business Saturday, and Cyber Monday flooded our inboxes and took over commercial breaks. As the holiday shopping season is in full swing, this is a good time to take a look at consumers' experience with mobile payments.

This morning, we will hear from witnesses representing a variety of innovative products and services in the mobile payments arena. This hearing is an opportunity to learn about the innovations that are available to consumers today and in the near future, but we recognize there are more exciting innovations on the horizon for payments, including mobile currencies, which may be a topic for another day.

Smartphones are increasingly an ever-present part of our lives and it's no surprise that they are also changing the way we shop for goods and services. You can shop on your tablet in front of the TV, compare prices on your phone as you browse in a store, and pay without ever pulling out your wallet. Consumers have access to more information and competitive options at the tip of their fingers during the busiest shopping season of the year.

There has not been this big of an upheaval in how consumers pay for goods and services—their groceries or a haircut—since computers replaced the old knuckle-busting manual imprinters in the 1980s.

In 2014, 22 percent of mobile phone owners reported making a purchase on their phone. Thirty-nine percent used their phones to make a purchase in a store.

When you find the perfect Christmas present, you may be able to pay by tapping your phone at checkout or clicking the PayPal Check Out button on a mobile Web site.

When you want to send your friend money for the concert ticket they bought for you, all you need is their email address or mobile phone number. These mobile payments options include protections not available with cash, and are easy to use for consumers who may be more likely to have their phone in their pocket than exact change.

Some basic questions remain top of mind for consumers when they think about mobile payments: "Are they safe?" "Can I use my phone?"

This hearing is an opportunity to hear from companies implementing the cutting edge technologies in mobile payments and how they are addressing these and other concerns raised by consumers.

Two of the security topics that are raised by mobile payments are authentication, how the device knows you have permission to make the payment with the device; and tokenization, protecting your payment data through the payment process.

As we all know, passwords are difficult. They are difficult to remember and difficult to keep straight which is why many people have the same password for multiple accounts. Mobile devices offer some alternatives to the traditional password that add an additional layer of protection for consumers.

Authentication is the process that a system uses to verify the identity of a person that wants to access that system. Your user name and password or passcode is the most typical authentication process used to log into a wide variety of Web sites.

Mobile devices have changed how people think about authentication. Fingerprints sensors and cameras are found on an increasing number of mobile devices. Now, instead of having to remember a separate password to unlock your phone or tablet, you may be able to use the fingerprint scanner and unlock the device with just a touch. This protects the information on your phone, including access to payment options.

Another security feature that is regularly brought up in discussions about mobile payments is tokenization. We're all familiar with the tokens you get at a fair or an arcade. Tokens in mobile payments are similar in concept—replacing the valuable currency or payment information with a code that is useless in another transactions if a hacker were to steal it.

As has been the case throughout history, technology has the potential to solve problems and improve our lives. Mobile payments are no exception to this trend.

I look forward to hearing from our witnesses about how they are leveraging a mix of technologies to provide an easy and secure experience for U.S. consumers as we make our way through the holiday shopping season.

Mr. BURGESS. And I will yield back the balance of my time and recognize the subcommittee ranking member, Ms. Schakowsky, 5 minutes for an opening statement, please.

OPENING STATEMENT OF HON. JANICE D. SCHAKOWSKY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Ms. SCHAKOWSKY. Thank you, Mr. Chairman, for holding this hearing and the series of hearings on disrupters. I just learned that at my bank, I can now make a deposit by taking a picture of the front and back of my check, and my bank will take it, although it doesn't account for my husband's really bad handwriting and says that it can't verify that the number I put in is the number he wrote on the check. That is a problem.

But I think this holiday shopping season, it is very important to hear from our witnesses about this important new technology. We do expect mobile payments to double from today to 2020. One of the fastest growing sectors of the U.S. economy, mobile payments do facilitate transactions with anyone from a food truck or farmers market seller or taxi driver, parking meter, and they have made buying and selling goods and services easier in many ways. But as this technology continues to expand, we definitely need to understand how the payment structure works, security, consumer protection vulnerabilities. How to address those issues is a responsibility of our subcommittee. We want to maximize benefits and minimize risks, obviously.

Mobile payment technologies rely on a number of nontraditional identifiers such as geolocation, purchase preference, phone numbers, email addresses. Those features can enhance protections against payment fraud. However, they can also put consumers at greater risk if they are unprotected or if their use extends beyond managing payments. With regard to electronic communications generally, we need to ensure that all of the players engaged in mobile payments, hardware and software developers, businesses, banks, credit unions, and credit card companies, are taking reasonable security measures to protect the information that they are handling. We also need to make sure that consumers know how these payment structures differ from more traditional transactions. Consumers need to know how consumer financial liability for these types of payments differs from those made using credit or debit

cards. They should also know how mobile payments can be used to cram consumers, running up bills that they never explicitly approved. And as the subcommittee responsible for consumer protection, we have an obligation to close those and other existing loopholes that leave consumers more vulnerable.

So I look forward to hearing from our witnesses, getting their perspectives on opportunities, challenges, and the way forward with regard to mobile payments.

And I yield back my time.

[The prepared statement of Ms. Schakowsky follows:]

PREPARED STATEMENT OF HON. JANICE D. SCHAKOWSKY

Thank you, Mr. Chairman, for holding today's hearing on mobile payments. I look forward to hearing from our witnesses on this important subject, which is all the more relevant during the holiday shopping season.

With mobile payments expected to double from today to 2020, this is one of the fastest-growing sectors of the U.S. economy. Mobile payments facilitate transactions with anyone from a food truck or farmers market seller to a taxi driver, and they have made buying and selling goods and services easier in many ways.

However, as this technology continues to expand, we need to understand how these payment structures work, what security and consumer protection vulnerabilities exist, and how to address those issues to maximize benefits while minimizing risks.

Mobile payment technologies rely on a number of non-traditional identifiers such as geolocation, purchase preferences, phone numbers and email addresses. Those features can enhance protections against payment fraud. However, they can also put consumers at greater risk if they are unprotected or if their use extends beyond managing payments.

As I have previously mentioned with regard to electronic communication generally, we need to ensure that all of the players engaged in mobile payments—hardware and software developers, businesses, banks, credit unions, and credit card companies—are taking reasonable security measures to protect the information they are handling.

We also need to make sure that consumers know how these payment structures differ from more traditional transactions. Consumers need to know how consumer financial liability for these types of payments differs from those made using credit or debit cards. They should also know how mobile payments can be used to "cram" consumers—running up bills that they never explicitly approve. And, as the subcommittee responsible for consumer protection, we have an obligation to close those and other existing loopholes that leave consumers more vulnerable.

I look forward to hearing our witnesses' perspectives on the opportunities, challenges, and the way forward with regard to mobile payments.

Mr. BURGESS. The Chair thanks the gentlelady. The gentlelady yields back.

The Chair recognizes the chairman of the full committee, Mr. Upton, 5 minutes for an opening statement, please.

OPENING STATEMENT OF HON. FRED UPTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. UPTON. Good morning. And today we continue our Disrupter Series. We have previously examined the Internet of things, the sharing economy, and, most recently, drones.

Today we discuss the growing trend of mobile payments. No matter where folks choose to travel or shop, whether it be in Michigan, the Nation, or even across the globe, their smartphones are ever-present, always at the ready to provide direction, daily news and scores, and even make payments. Early estimates show that, for the first time ever, more people shopped online than in stores over the Thanksgiving holiday. Cyber Monday estimates are still being

tallied, but we are no doubt seeing a fundamental shift in how people are buying the goods and services available to them throughout our economy. Consumers have more choices than ever before about when and where to shop. These choices open up opportunities for innovations to take root and spread throughout the economy.

We have seen this sort of disruption throughout this series of hearings, and mobile payments are certainly no different. They are impacting how the Internet of things and the sharing economy develops. The Disrupter Series remains important as we work to better understand how innovations impact consumers, job creation, and our economy as a whole.

Mobile payment technologies have opened up opportunities for individuals and businesses alike, so businesses small and large can benefit from these disruptions as we have seen with a hardware like Square and software like Venmo, which make payments easier for small businesses and between respectively. These are just two examples in an ecosystem that is bursting with growth as more and more Americans get smartphones, tablets, and other mobile devices. New technologies and competition are responding to consumer needs.

Mobile payment innovation is happening all over the country. However, adoption across the ecosystem continues to be a challenge that all businesses in this space are working to address. There are a lot of facets to the mobile payment space, and I am pleased that today we are going to learn more about the options that consumers have, particularly how these options can and will continue to improve security for consumers and job creators.

[The prepared statement of Mr. Upton follows:]

PREPARED STATEMENT OF HON. FRED UPTON

Today we continue our Disrupter Series. We have previously examined the Internet of Things, the Sharing Economy, and most recently drones—and today we discuss the growing trend of mobile payments. No matter where folks choose to travel or shop, in Michigan, the Nation, and even abroad, their smartphones are ever present, always at the ready to provide directions, daily news and scores, and even make payments.

Early estimates indicate that for the first time ever, more people shopped online than in stores over the Thanksgiving holiday weekend. The Cyber Monday estimates are still being tallied, and we are no doubt seeing a fundamental shift in how people are buying the goods and services available to them throughout our economy.

Consumers have more choices than ever about when and where to shop. These choices open up opportunities for innovation to take root and spread throughout the economy.

We have seen this sort of disruption throughout this series of hearings and mobile payments are no different. They are impacting how the Internet of Things and the sharing economy develop. The Disrupter Series remains important as we work to better understand how innovations impact consumers, job creation, and our economy as a whole.

Mobile payment technologies have opened up opportunities for individuals and businesses alike. Businesses small and large can benefit from these disruptions as we have seen with hardware like Square and software like Venmo, which make payments easier for small businesses and between friends, respectively. These are just two examples in an ecosystem that is bursting with growth as more and more Americans get smartphone, tablets, and other mobile devices.

New technologies and competition are responding to consumer needs. Mobile payment innovation is happening all over the country. However, adoption across the ecosystem continues to be a challenge that all businesses in this space are working to address.

There are a lot of facets to the mobile payments space and I am pleased that today we will learn more about what options consumers have and particularly how those options can and will continue to improve security for consumers and job creators.

Mr. UPTON. And I yield the balance of my time to Marsha Blackburn.

Mrs. BLACKBURN. Thank you, Mr. Chairman.

And I am so appreciative that we are doing this hearing today, and I thank our witnesses. You all are the experts, and we have plenty of questions that we are going to have for you. Wireless and mobile devices and quick purchases are changing things. And this past weekend, my 6-year-old grandson got into the app store on my iPhone, found something that he wanted to buy, handed me the phone and said, "Marcia, you need to pay for this," and, of course, I did not. But I use this illustration to make a point of the simplicity and also the assumption of our kids and grandkids that it is going to be at the scan of a screen or a touch of a button or with great ease that you are going to be able to make these purchases on the go, in realtime, paid in realtime, and with great convenience and security.

And that is where much of our focus is going to be, whether it is the multifactor identification or tokenization or what I want to hear from you, the "what is next?" Where do you think we are going with this? Because convenience, yes, people want it. Security, they are going to demand it because they want to be able to protect their virtual presence online just as they are able to protect their presence in the brick-and-mortar relationship with those that they are choosing to do business with. So I thank you for the time that you are going to spend with us today, your preparation in coming to the committee, and I look forward to your thoughts on what is next.

I yield back.

Mr. BURGESS. The gentlelady yields back. The Chair thanks the gentlelady.

The Chair recognizes the gentleman from New Jersey, the ranking member of the full committee, 5 minutes for an opening statement, please.

OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

Mr. PALLONE. Thank you, Chairman Burgess.

During today's hearing, we will discuss the new ways consumers are paying for goods and services through their mobile devices. At a time when it seems like virtually everything is tied to our smartphones, it should come as no surprise that we are now able to store credit cards electronically, transfer funds directly to our peers, and make purchases by simply tapping our phones to a terminal at the point of sale.

These exciting innovations hold promise for consumers. Imagine the convenience of being able to send money instantly to a friend or family member regardless of location or proximity to an ATM. For consumers who forget their credit cards at an outing, a mobile peer-to-peer payment could be the difference between being

squared away and an IOU. The ability to store credit cards in your phone may also offer consumers some peace of mind that in the event of a lost or stolen phone, their information is safe behind a pass code, and a physical card is not compromised.

Perhaps most encouraging for consumers with limited or no access to a bank, mobile payments can be a welcome alternative for purchasing the goods and services they need. For example, the use of mobile payments has skyrocketed in Kenya, where access to banking is quite limited.

With all these new products that involve consumers' personal information, however, privacy concerns must be raised. In general, mobile payment apps can access a wealth of personal data through a user's smartphone, such as phone numbers, geolocation, email addresses, and detailed purchase histories. Consumers do not know who has access to their information or with whom it is shared. This data may be used in ways the consumer never intended, including by merchants sending unwanted advertising tailored to consumers through their mobile devices. And that personal information could also be sold, so consumers' location and other private matters are shared with the highest bidder. That is why privacy protection should be baked into these new mobile pay applications.

It is also important that consumers are ensured a secure transaction through a mobile payment system. As with any mobile device or application, digitally stored or transmitted information is hackable. With the major data breaches of the past few years still fresh in consumers' minds, mobile payment users will understandably be hesitant about using an app if there is no protection from hackers who may try to intercept their personal information. It has been made clear through this series of hearings on disrupters, innovation, and consumer protection must go hand-in-hand for these new technologies to flourish. Mobile payments present an exciting opportunity to make e-commerce a more seamless experience for consumers, and I look forward to hearing from today's witnesses on this topic.

Thank you, Mr. Chairman, and I yield back.

[The prepared statement of Mr. Pallone follows:]

PREPARED STATEMENT OF HON. FRANK PALLONE, JR.

Thank you Chairman Burgess. During today's hearing, we will discuss the new ways consumers are paying for goods and services through their mobile devices.

At a time when it seems like virtually everything is tied to our smartphones, it should come as no surprise that we are now able to store credit cards electronically, transfer funds directly to our peers, and make purchases by simply tapping our phones to a terminal at the point of sale.

These exciting innovations hold promise for consumers. Imagine the convenience of being able to send money instantly to a friend or family member regardless of location or proximity to an ATM. For consumers who forget their credit card on an outing, a mobile peer-to-peer payment could be the difference between being squared away and an I.O.U.

The ability to store credit cards in your phone may also offer consumers some piece of mind that, in the event of a lost or stolen phone, their information is safe behind a passcode and a physical card is not compromised.

Perhaps most encouraging, for consumers with limited or no access to a bank, mobile payments can be a welcome alternative for purchasing the goods and services they need. For example, the use of mobile payments has skyrocketed in Kenya, where access to banking is quite limited.

As with all new products that involve consumers' personal information, however, privacy concerns must be raised.

In general, mobile payment apps can access a wealth of personal data through a user's smartphone, such as phone numbers, geolocation, email addresses, and detailed purchase histories. Consumers do not know who has access to their information or with whom it is shared. This data may be used in ways the consumer never intended, including by merchants sending unwanted advertising tailored to consumers through their mobile devices. That personal information also could be sold, so consumers' location and other private matters are shared with the highest bidder. That is why privacy protections should be baked into these new mobile pay applications.

It is also important that consumers are ensured secure transactions through a mobile payment system. As with any mobile device or application, digitally stored or transmitted information is hackable. With the major data breaches of the past few years still fresh in consumers' minds, mobile payment users will understandably be hesitant about using an app if there is no protection from hackers who may try to intercept their personal information.

It has been made clear through this series of hearings on disrupters, innovation and consumer protection must go hand in hand for these new technologies to flourish.

Mobile payments present an exciting opportunity to make e-commerce a more seamless experience for consumers, and I look forward to hearing from today's witnesses on this topic. Thank you and I yield back.

Mr. BURGESS. The gentleman yields back. The Chair thanks the gentleman.

And this concludes Member opening statements. The Chair would remind Members that, pursuant to committee rules, all Members' opening statements will be made part of the record.

And we do want to thank our witnesses for being here this morning and taking time to testify before the subcommittee. Our witness panel today—and we do have a good and great group—our witness panel for today includes Mr. John Muller, the senior vice president for global payments policy at PayPal; Ms. Jessica Deckinger, chief marketing officer at the Merchant Consumer Exchange; Ms. Sarah Jane Hughes, university scholar and fellow in commercial law at the Indiana University School of Law; and Mr. Sang Ahn, chief commercial officer at U.S. Samsung Pay.

We appreciate all of you being with us this morning. We will begin the panel with you, Mr. Muller.

And each you of will be recognized for 5 minutes for a summary of your opening statement.

Mr. Muller, you are recognized.

STATEMENTS OF JOHN MULLER, VICE PRESIDENT, GLOBAL PAYMENTS POLICY, PAYPAL; JESSICA E. DECKINGER, CHIEF MARKETING OFFICER, MERCHANT CUSTOMER EXCHANGE; SARAH JANE HUGHES, UNIVERSITY SCHOLAR AND FELLOW IN COMMERCIAL LAW, MAURER SCHOOL OF LAW, INDIANA UNIVERSITY; AND SANG W. AHN, CHIEF COMMERCIAL OFFICER, U.S. SAMSUNG PAY, SAMSUNG ELECTRONICS AMERICA

STATEMENT OF JOHN MULLER

Mr. MULLER. Thank you, Mr. Chairman and Ranking Member Schakowsky, and the other members of the committee. Thank you for the opportunity to testify on behalf of PayPal. My name is John Muller, and I am vice president of payments policy for PayPal. And PayPal has been involved in mobile payments now for 16 years and started with the cutting-edge payments mobile device of its time,

which was the PalmPilot, you may remember, the personal digital assistant without phone capability, but a very portable device. And PayPal was actually built to beam payments from one PalmPilot to another. At that point, we quickly realized that more people had email and Internet access than owned a palm pilot palm pilot, but we have now come back full circle to a focus on mobile payments to the point that last year we processed 1 billion payments from mobile devices all around the world, and just in the last quarter of this year, the growth rate continues, and we processed 345 million mobile payments. I have some more information on PayPal in the prepared statement, so I wanted to shift a little bit and just make a few high-level points about mobile payments and where we stand today.

One point is payments follows commerce, and it follows where people spend their time. Very few people, maybe the people on this panel excepted, make a payment just for fun or just to try it out. There is always a purpose behind it, and for most of us, the purpose is commerce, or the purpose might be to pay back a friend. And increasingly, we are doing our shopping on mobile devices, and we have our mobile devices with us when we are out with a friend or contacting a friend, so it is only natural for payments to be part of that broader mobile experience.

Another point is that payment has been mobile for quite some time. There are few things more portable than paper currency and coins or a plastic card. What is really new about the new generation of mobile payments is the opportunity for all of us in the payments industry to take advantage of what the technology makes available, namely increased security through things like the device identifier or geolocation on the device or biometrics on the device—the thumbprint being the first live version of that, but certainly more to come in that arena. And then, to that security, add a better user experience compared to just paying with cash or a card: things like automatically recognizing my loyalty program, giving me points, giving me choice of funding methods. So if I have a card, a plastic card, then I have to use that card. If I have a digital wallet like PayPal or the other wallets, I can use my mobile device in realtime to switch among all the different payment methods that I have available. So those are some of the reasons why we see the growing popularity of mobile payments.

Another point I wanted to make is we often use the term broadly mobile payments, and it really covers to a large degree three different fields. One—and certainly the one that predominates for PayPal and many other payment companies—is using the mobile device as a substitute for what a few years ago would be a transaction on the laptop or desktop computer, so just communicating with a new kind of device but really very similar to the kind of e-commerce transactions we were doing in the early 2000s.

The second type—and certainly the one that gets a great deal of attention for good reason now because the opportunity to touch not just e-commerce but physical commerce—is using the phone as a substitute for the plastic card and paying at a physical point of sale.

And then the third type, certainly not to diminish it in any way, equally important, is using the mobile device as a way of enabling

businesses, mostly small businesses, to accept cards and other payment methods electronically in a mobile business environment, whether it is a food truck or a farmers market or any of the other many opportunities that small businesses use for devices, attaching a small reader to their device and using it usually to swipe a card or enter another payment method. Companies like Square and PayPal have made that available to small businesses all over the country. And all of those are different types of mobile payments, but it is important to recognize that there are distinctions among the three.

And then, finally, also important to recognize that the field is already regulated. We have to give credit to the drafters in particular of the Electronic Fund Transfer Act. When they created consumer protections for what at the time was primarily the ATM card quite a few years ago, they drafted the statute in terms of access devices and financial accounts, not limited to plastic cards or any other kind of specific technology. So an access device can be a password or a phone or any other device, and the consumer protections remain in place supplemented by the zero liability programs that Visa and MasterCard and PayPal all offer to buyers. So I just wanted to make those broader points.

And, with that, I will conclude my remarks. Thank you, and I look forward to the questions.

[The prepared statement of Mr. Muller follows:]

TESTIMONY OF

John Muller

Vice President, Global Payments Policy

PayPal, Inc.

BEFORE THE

United States House of Representatives

Committee on Energy and Commerce

Subcommittee on Commerce, Manufacturing, and Trade

"The Disruptor Series: Mobile Payments"

PRESENTED

Rayburn House Office Building, Room 2322

December 1, 2015

10:15 AM

Chairman Burgess, Ranking Member Schakowsky, and Members of the Subcommittee: Thank you for the opportunity to testify this morning on the role that mobile payments play in disrupting today's financial services landscape.

My name is John Muller and I am the Vice President of Global Payments Policy for PayPal, Inc. PayPal is a leading payments company, with more than 173 million active users around the world. From starting with customers beaming payments on their Palm Pilot devices in 1999 to 345 million payments on mobile devices in the third quarter of this year, PayPal continues to transform how people shop and pay.

PayPal was founded with the simple goal of making sending a payment faster, easier, and more secure. The company's products and technologies have evolved to match the growing trend towards mobile payments from both a consumer and a merchant platform. I'd like to give the subcommittee some background on PayPal and our products, and explain why and how mobile technologies are disrupting traditional payment options.

Mobile technologies powered by the internet enable us to purchase and sell goods or services anywhere, all with the touch of a button. The adoption of mobile phones and other mobile devices is the fastest mass adoption of technology in history. Because of mobile technology, people all over the world can move their offline businesses to a global marketplace almost instantly. This represents a seismic shift in the world of commerce, and mobile is just the beginning of this wave. We are seeing a proliferation of connected devices. By 2020, there will be more than 50 billion "things" connected to the

Internet.[1] The more connected we are, the easier it is for people to make purchases and transactions.

PayPal's Position in Mobile Payments

PayPal offers consumers a "digital wallet" that connects into and leverages traditional payment networks, enabling PayPal's users to send and receive both personal and commercial payments in a safe, secure, and efficient manner. Because PayPal is hardware-agnostic, it can operate in virtually any digital ecosystem.[2]

Most of our customers still open their account and transact using a traditional desktop or laptop computer, but our mobile app and mobile-optimized Website gives them the choice to access the full power of their online account in their mobile device. We also help merchants, especially small merchants, optimize their checkout pages for mobile access. So with the touch of a button on your smartphone, you can pay directly at participating retailers, check your account balance, and send money to individuals in more than 100 countries around the world.

Physical money is digitizing right in front of our eyes. 40% of the money passing through consumers' wallets today is in the form of either checks or cash. That number is predicted to drop to 5% by 2017.[3]

---

[1] Evans, D. (April 2011). The Internet of Things, How the Next Evolution of the Internet is Changing Everything. Retrieved November 24, 2015, from: https://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[2] Weill, P. and Woerner, S. (June 16 2015). Thriving in an Increasingly Digital Ecosystem. Retrieved November 23, 2015, from http://sloanreview.mit.edu/article/thriving-in-an-increasingly-digital-ecosystem/.

[3] Schulman, D. (March 04 2015). Morgan Stanley Technology, Media & Telecom Conference. Retrieved November 23, 2015, from: http://www.nasdaq.com/aspx/call-transcript.aspx?StoryId=2973946&Title=ebay-s-ebay-management-presents-at-morgan-stanley-technology-media-telecom-conference-transcript-#ixzz3sSjgm6HY.

The convenience brought forth by mobile payment technology has caused it to be adopted by both merchants and consumers at huge scale. Out of the 4 billion transactions PayPal processed last year, 1 billion were made on a mobile device. This growth is continuing – in the most recent quarter of this year, we processed 345 million mobile payments, up 38% year over year. Mobile payments are becoming the technology of choice for people across the world.

Mobile as a Disruptor

In order to understand mobile technologies as disruptors, we must recognize that ecommerce is still in its earliest stages. Ecommerce accounts for only 10% of all commerce, but it is growing at a rate of 17% a year.[4] We believe that the offline marketplace is a ripe opportunity for PayPal and other mobile payment providers to penetrate. As consumers and merchants shift to mobile, they are showing that they want to use mobile devices to access traditional financial mechanisms such as bank accounts and credit cards, and potentially to access new payment methods such as prepaid cards, digital wallet balances and digital currencies.

Protecting Consumers and Their Data

Today, the financial services sector is primed for the transition to mobile and frictionless payments. The digitization of money, the near ubiquity of Internet access, and the availability of mobile phones have created the ideal circumstances for companies to examine ways to reduce costs and burdens associated with transferring money through the system. More importantly, these developments have also provided people easier and

[4] Schulman, D. (March 04 2015). Morgan Stanley Technology, Media & Telecom Conference. Retrieved November 23, 2015, from: http://www.nasdaq.com/aspx/call-transcript.aspx?StoryId=2973946&Title=ebay-s-ebay-management-presents-at-morgan-stanley-technology-media-telecom-conference-transcript-#ixzz3sSjgm6HY.

cheaper ways to manage their money. At the same time, these developments have increased the need for security to protect users' information from hackers and fraud. At PayPal, part of our core corporate mission is to work to make technology the vehicle for delivering a great consumer experience – complete with built-in robust protections.

PayPal was founded by a computer security expert, Max Levchin, partly as a way of demonstrating that payments could be done securely online in the early days of the Internet. For more than 15 years, we at PayPal have strived to be at the cutting edge of cyber security technology. According to Javelin Research[5], PayPal is the most trusted partner by consumers for mobile payments—ahead of traditional credit card providers and other technology companies. PayPal is designed from the ground up to be one of the safest and most secure ways to send money online. For consumers, one of the fundamental benefits of paying with PayPal is that we process your payment without revealing your financial account information to the merchant. When you choose to pay with PayPal, you provide the merchant only your name and email address and (for physical goods transactions) your shipping address. We encrypt the rest of your information and then send the payment to the merchant. For our community of merchants, because they never receive the customer's credit card or bank account information, they are spared the burden of storing and managing this information securely. This early form of tokenization that we started 16 years ago continues to be the foundation of our customer protection.

[5] Monahan, M. (October 2013) 2013 Gang Of Five: Apple, Google, Amazon, Facebook, and PayPal-eBay: Threat of the Mobile Wallet Disruptors. Retrieved November 23, 2014, from: https://www.javelinstrategy.com/brochure/298.

Security and Innovation in Mobile Payments

At PayPal we believe our customers' security is a top priority. To provide you an example of this importance, I'd like to discuss one of the ways we are using mobile devices to enhance the effectiveness of our customer protection.

Mobile Authentication

Online businesses have typically achieved authentication through a combination of username and passwords, supplemented in the background by risk models looking for anomalies in the customer's log-in or transaction details. This approach has been the standard on desktop computers since before PayPal helped pioneer digital commerce and online shopping experiences, and this is still the way that most users understand authentication. Biometric authentication features on mobile devices are radically changing this model and subsequently, minimizing damage done in a breach or hack. Through PayPal's leadership and collaboration with Samsung and the FIDO Alliance (Fast Identity Online), PayPal was the first payment company to introduce fingerprint biometric payment authentication on Android mobile devices. Our technique uses a unique ID that is tied to the device in conjunction with biometric data, with the data stored on the device, not stored in any central database. Pairing up device and transaction location is a valuable feature when assessing transactions for fraud, and reduces the chance of stolen data being used fraudulently. When the geolocation feature is enabled on a mobile device, suspicious behavior such as fraudulent activity and account takeovers are easier to identify. Imagine that charges from a payment account are attempted at a physical store in New York City but PayPal knows the account holder is located in San

Francisco due to a very recent transaction on her mobile device. The location disparity allows businesses to quickly identify illegitimate transactions.

When using mobile devices, there is some confusion about the way that the transactions occur. The online segment of the mobile transaction is the authentication piece only- the user's credit card numbers are never exposed to the device. Instead of storing financial and identity information on mobile devices, PayPal's infrastructure is built so that critical account and payment information is stored in the cloud. This means that the three elements required to make a mobile transaction: the device, the fingerprint, and the credit card data, never reside in the same location at the same time. These elements coupled with geolocation reduce the scalability of fraudulent transactions.

Mobile Enabling Financial Inclusion

At PayPal we've learned that mobile technologies can serve as a tool for financial inclusion by harnessing the power of mobility to "bring the institutions to the person". According to the Corporation for Enterprise Development (CFED), there are 9 million unbanked households in the United States. Most unbanked cities in America are in very small and rural towns - 36 of the 100 most unbanked places are in Texas, 17 are in Mississippi, and 10 are in Arizona.[6]

The residents in these rural communities face limited options when it comes to managing and moving their money. In order to make a deposit or withdrawal, people must travel long distances to find a bank branch or ATM location, and when they do, they can be hit with high fees associated with their transactions. At PayPal our goal is to offer another solution, an alternative technology to meet their needs, which includes mobile

[6] Geiling, E. (2015). The Most Unbanked Places in America. Retrieved October 26, 2015, from https://cfed.org/newsroom/experts/ethan_geiling/the_most_unbanked_places_in_america/.

payments. PayPal's President and CEO, Dan Schulman has made financial inclusion a high priority of our company. The prominence of cell phones and access to broadband has positioned mobile to play a role in filling the gap for the 20% of the population that sit outside the traditional banking system. As a starting point, we have expanded the availability of prepaid cards as a method for funding PayPal transactions. As the committee continues to discuss mobile payments, we urge you to keep in mind the connection between broadband and mobile broadband deployment and its impact on members of underbanked communities.

Conclusion

Thank you for the opportunity to testify today. Although PayPal has been leading the mobile payments space for a number of years we still think of ourselves as an innovator. Having recently spun-off from eBay Inc. earlier this year, we like to say that we are a 17 year-old start-up. We also support other start-up businesses through programs like Startup Blueprint, which offers business advice and free processing on the first $50,000 of payments to selected startup companies, and PayPal Working Capital, which offers working capital loans to qualified merchants through a bank partner. However, like any start-up we are guided by core commitments, which in our case include building a trusted relationship with our consumers based on our ability to protect their data and provide them with as frictionless an experience as possible.

I look forward to answering any questions you may have.

Mr. BURGESS. The Chair thanks the gentleman.

And, Ms. Deckinger, you are recognized for 5 minutes.

STATEMENT OF JESSICA E. DECKINGER

Ms. DECKINGER. Thank you, Mr. Chairman, Ranking Member Schakowsky, and distinguished members of the subcommittee. Thank you for the opportunity to testify on behalf of Merchant Customer Exchange for MCX. We appreciate the invitation to appear before the subcommittee to discuss the rapidly developing and evolving mobile payment space. The subcommittee's interest in the topic is welcome as mobile payment solutions are rapidly moving to the forefront of consumer technology innovations, both in the United States and globally.

Who is MCX? So the Merchant Customer Exchange was founded by a leading group of U.S. merchants in 2012 to create a broadly accepted mobile commerce platform. MCX's members include retail leaders in the big box, convenience, fuel, grocery, quick service, full dining, and specialty retail travel categories. MCX is focused on creating convenience for consumers by allowing them to securely pay for goods and services from their handheld mobile device while also providing opportunities for merchants to directly connect with consumers to provide offers, loyalty programs, and more direct interaction with the merchants they shop with. I prepared a short video for you to get a sense of what CurrentC, our app, is all about.

[video shown.]

Ms. DECKINGER. This new network will benefit a wide range of consumers in three ways: One, delivering a better shopping and payment experience by enabling customers to interact directly with merchants through virtually any smartphone; two, safeguarding consumers and merchants by maintaining the direct relationship that merchants have with customers and protecting customer data; three, bringing balance to the payments ecosystem.

Together MCX's member companies process in excess of $1.2 trillion in payments annually, giving MCX scale and ubiquity that will allow consumers to use their smartphones wherever they may shop. MCX brings together the best-in-class technology and mobile payments partners to create an unparalleled network in the mobile space. To achieve this goal, MCX has launched its own proprietary application called CurrentC that can be downloaded to any smartphone a customer may choose.

We have conducted private rollouts with leading retailers and their employees, and as of September 15, 2015, this year, we are currently in a public beta operating in Columbus, Ohio. The purpose of our beta in Columbus is to gather additional learnings from consumers and merchants to continue to refine and improve the product to meet the needs of both consumers and the merchants. Expansion of the rollout will continue as additional merchants and partners go live in Columbus through the balance of 2015 with national public availability currently anticipated in 2016.

Today consumers' experiences with payments can differ fairly drastically depending on where they are shopping. At a fuel station, they may be asked to dip their card or type their ZIP Code in to begin fueling. At a sit-down dining establishment, consumers wait for the server before physically relinquishing their card to the

establishment. Other merchants have more self-service experience, where consumers swipe their own cards at checkout. And we have specifically designed our technology platform to support the best, most progressive technologies to deliver an optimal payments experience at any merchant to serve their customers in the best way possible.

To deliver that best consumer experience at merchants, we are leveraging several types of technology solutions. We remain open to new technologies and are always looking to source the very best options for consumers and our merchants. At present, we are working with several different innovative technologies, including QR codes, Bluetooth low-energy beacons, and geolocation, providing the best user experience regardless of location.

Fundamentally the current payment system works well from a consumer's perspective. Swiping a credit or debit card is widely accepted, easy to do, and familiar. MCX and its merchants are focused on providing consumers new, more convenient, and more rewarding, and safer ways to shop.

CurrentC provides incentives to consumers in four important ways. Wide acceptance: Our owner-merchants already include national leading retailers and regional leaders in large-format, convenience, pharmacy, fuel, drug, grocery, quick, full-service dining, specialty retail, and travel categories. We are focused on acceptance in the places where consumers shop every day. Developing that network will give consumers the ability to shop with frequency and to develop muscle memory using CurrentC, allowing it to replace the card swipe over time while providing additional security and convenience.

At MCX, we are technology agnostic. CurrentC is available on any smartphone regardless of model. We believe the consumer should have the convenience of mobile payments regardless of their hardware choices. And because CurrentC is cloud-based, it is easily transferrable should a consumer choose to change their chosen mobile device solution.

We have also partnered with merchants to provide CurrentC payments network to consumers within the merchant's own priority apps. This means a consumer can choose to access CurrentC directly or have the ability to garner the same benefits if they wish to use the merchant app which they use every day.

Merchants value their relationships with their customers and want to enhance those relationships, adding value that motivates consumers to shop in store with faster, safer, and more secure way to transact. CurrentC delivers by including consumer loyalty cards and accounts, empowering consumers to apply offers, coupons, promotions, and when they pay in a single transaction. Our solution is designed to combine all those benefits instantaneously together in one QR code read so that a consumer no longer has to remember a phone number to activate their loyalty account or use their key chain to get discounts.

Because CurrentC is tied directly into the POS terminals at our merchants, we have the ability to deliver additional benefits, such as item level coupons, which alleviates the need to either clip or carry paper coupons or discount offers, all in an effort to provide

flexibility, choice, and the ability to benefit from offers and loyalty directly from their handheld device.

Currently, we are testing several discount and incentive programs in Columbus. Two of our most popular are a coupon for a free Frosty, which is an ice cream cone, with every purchase at Wendy's, and a $5 bonus extra care box with a first purchase using CurrentC at CVS. What we are seeing is that to the average consumer, these are tangible motivators.

Consumers will have the freedom to pay using a variety of financial accounts, including personal checking accounts, merchant gift cards, private label credit and debit cards, and general purpose credit and debit cards.

MCX recently signed a partnership with JPMorgan Chase which will increase options available in the CurrentC wallet by enabling Chase customers to use their Chase cards wherever CurrentC is accepted. It is anticipated that additional general purpose credit and debit cards will be available in the future.

At MCX, we are always open to adding new forms of payment that will provide greater convenience to consumers and allow them to realize the benefits and incentives of moving to paying with their favorite merchants using CurrentC mobile payments platform. At MCX, we are focused on leveraging innovative and secure technology.

Consumers are inundated with headlines around data breaches and identity theft. As a result, they have become more aware of the vulnerability of various payment methods and technology. However, many consumers remain in the dark about how to leverage the latest security technologies in their everyday lives. At MCX, we believe it is incumbent on mobile payment technologies like ours not only to use the latest security technology but to help educate consumers on how it is working for them. We are leveraging cloud technology to avoid storage of any sensitive consumer information on the phone or transferred at the POS. Our app uses secure dynamic tokens uniquely generated for each individual transaction to facilitate transactions instead of constantly passing data between the consumer, merchant, and financial institution. In the simplest term, using a dynamic token means that the consumer can feel assured that their personal financial information or payment information is never stored on the device, is never stored on the merchant POS, and even if the dynamic token was stolen, it is worthless because it can never be used again.

CurrentC was designed to ensure consumers are in control of their own personal security. It provides visual evidence to demonstrate that our security measures are working for them.

Mr. BURGESS. Ms. Deckinger, let me ask you to please wrap up. We have other witnesses to hear from.

Ms. DECKINGER. OK. Thank you. I will just finish this section and then finish. Our registration process includes several security questions, a four-digit PIN, and consumers can disable their phones easily and quickly.

We want to reiterate our appreciation for your interest in mobile payments technologies and providing Merchant Customer Exchange the opportunity to share about our innovation and currently underway in the mobile payments space. We truly believe that mo-

bile payments will provide a better opportunity for merchants and consumers to experience an improved experience overall. Thank you.

[The prepared statement of Ms. Deckinger follows:]

MCX MERCHANT CUSTOMER EXCHANGE

PREPARED STATEMENT OF MERCHANT CUSTOMER EXCHANGE (MCX)

For the

COMMITTEE ON ENERGY AND COMMERCE OF THE UNITED STATES HOUSE OF REPRESENTATIVES SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

On

THE DISRUPTER SERIES: MOBILE PAYMENTS

Jessica E. Deckinger
Chief Marketing Officer
Merchant Customer Exchange

December 1, 2015
Prepared Statement of Jessica E. Deckinger

Chairman Burgess, Ranking Member Schakowsky, and distinguished members of the Subcommittee, thank you for the opportunity to testify on behalf of Merchant Customer Exchange, LLC or MCX. We appreciate the invitation to appear before the Subcommittee to

discuss the rapidly developing and evolving mobile payments space. The Subcommittee's interest in the topic is welcome as mobile payment solutions are rapidly moving to the forefront of consumer technology innovations both in the United States and globally.

Who is MCX?

The Merchant Customer Exchange ("MCX") was founded by a leading group of U.S. merchants in 2012 to create a broadly accepted consumer mobile commerce platform. MCX's members include retail leaders in the big-box, convenience, drug, fuel, grocery, quick and full-service dining, specialty-retail and travel categories. MCX is focused on creating convenience for consumers by allowing them to securely pay for goods and services from their handheld mobile device while also providing opportunities for merchants to directly connect with consumers to provide offers, loyalty programs, and more direct interaction with the merchants they shop with.

This new network will benefit a wide range of consumers in three basic ways:

(1) Delivering a better shopping and payment experience by enabling customers to interact directly with merchants through virtually any smartphone

(2) Safeguarding consumers and merchants by maintaining the direct relationships that merchants have with customers and protecting customer data

(3) Bringing balance to the payments ecosystem

Together, MCX's member companies process in excess of $1.2 trillion in payments annually, giving MCX scale and ubiquity that will allow consumers to use their smartphone wherever they

may shop. MCX also brings together the best in class in technology and mobile payments partners, to create an unparalleled network in the mobile space.

To achieve this goal, MCX has launched its own proprietary application (or "app") called "CurrentC" that can be downloaded to any smartphone a consumer may choose. We have conducted private rollouts with leading retailers and their employees, and, as of September 15, 2015, are currently in a public beta operating in Columbus, OH. The purpose of our beta in Columbus is to gather additional learnings from consumers and merchants to continue to refine and improve our product to meet the needs of both consumers and merchants. Expansion of the rollout will continue as additional merchant partners go live in Columbus throughout the balance of 2015, with national public availability currently anticipated in 2016.

Today, consumer's experiences with payments can differ fairly drastically depending on where they are shopping. At a fuel station, they may be asked to dip their card and type in their zip code to begin fueling. At sit down dining establishments, consumers wait for a server before physically relinquishing their card. Other merchants have more of a self-service experience, where consumers swipe their own cards at checkout.

We have specifically designed our technology platform to support the best, most progressive technologies to deliver an optimal payments experience at any merchant to serve their customers in the best possible manner. To deliver that best experience at each merchant, we are leveraging several types of technology solutions. We remain open to new technologies, and are always looking to source the best options for consumers and our merchants.

Providing Consumer Benefit

Replacing more than the swipe

Fundamentally, the current payments system works well from a consumer's perspective. Swiping a credit/debit card is widely accepted, easy to do and familiar. MCX and its merchants are focused on providing consumers new more convenient, more rewarding, and safer way to shop.

CurrentC provides incentives to consumers in four important ways:

Wide acceptance: Our owner-members already include national and regional leaders in the large-format, convenience, pharmacy, fuel, grocery, quick- and full-service dining, specialty-retail and travel categories. We are focused on acceptance in the places where consumers shop every day. Developing that network will give consumers the ability to shop with frequency, and to develop the "muscle memory" of using CurrentC, allowing it to replace the card swipe over time while providing additional security and convenience.

Accessibility: At MCX, we are technology agnostic. CurrentC is available on virtually any smartphone, regardless of model. We believe that consumers should have the convenience of mobile payment regardless of their hardware choices; and because CurrentC is cloud based, it is easily transferable should a consumer change their chosen mobile device solution. We have also partnered with merchants to provide the CurrentC payments network to consumers within the merchants' own proprietary "apps". This

means a consumer can choose to access CurrentC directly or have the flexibility to garner the same benefits if they wish to use the merchant app to shop and pay.

Personalized benefits: Merchants value their relationships with their customers, and want to enhance those relationships, adding value that motivates consumers to shop in store with a faster, safer and more secure way to transact. CurrentC delivers by including consumer loyalty cards/accounts, empowering consumers to apply offers, coupons, promotions, whenever they pay in one single transaction. Our solution is designed to combine all of those benefits instantaneously, together, in one QR code read, so that a consumer no longer has to remember a phone number to activate their loyalty account or use their key chain to get discounts. Because CurrentC is tied directly into the POS terminals at our merchants, we have the ability to deliver additional benefits such as item-level coupons, which alleviates the need to either clip and carry paper coupons or discount offers – all in an effort to provide consumers flexibility, choice, and the ability to benefit from the offers and loyalty directly from their handheld device. -At present, we are in market with several innovative technologies, including QR Codes, Bluetooth Low Energy, and Geo Location, providing the best user experience regardless of location.

Broad payment options: Consumers will have the freedom to pay using a variety of financial accounts, including personal checking accounts, merchant gift cards, private label credit and debit cards, and general purpose credit and debit cards. MCX recently signed a partnership with JP Morgan Chase, which will increase the options available in the CurrentC wallet. It is anticipated that additional general-purpose credit and debit

cards will be available in the future. At MCX, we are always open to adding new forms of payment that will provide greater convenience for consumers and allow them to realize the benefits and incentives of moving to paying in their favorite merchants using the CurrentC mobile payments platform.

Innovative and Secure Technology

Consumers are inundated with headlines around data breaches and identity theft. As a result, they have become more aware of the vulnerability of various payment methods and technologies. However, many consumers remain in the dark about how to leverage the latest security technologies in their every day lives. At MCX, we believe it is incumbent on mobile payments technologies like ours not only to use the latest security technology, but to help educate consumers about how it is working for them.

We are leveraging cloud technology to avoid storage of any sensitive consumer information on the phone or transferred at POS. Our app uses secure dynamic tokens, uniquely generated for each individual transaction, to facilitate transactions instead of constantly passing the data between the consumer, merchant and financial institution. In the simplest terms, using a "dynamic token" means that consumers can feel assured that their personal financial information or payment information is never stored on the device, is never stored on the merchant POS, and even if the dynamic token was stolen, it is worthless because it cannot ever be used again.

CurrentC was designed to ensure consumers are in control of their personal security, and

provides visual evidence to demonstrate that our security and protective measures are working for them.

(1) Our registration process includes several security questions which are used as identifiers should consumers get "locked out" of the app.

(2) Consumers are asked to create and use a customized 4-digit personal PIN to unlock the app every time they exit and re-open it. A lost or misplaced phone can't be used to pay, because the 4 digit personal PIN needs to be activated for each and every payment transaction.

(3) We provide an easy to follow process to disable a phone from CurrentC should a consumer lose their mobile device and wish to shut their account down for peace of mind.

CurrentC was also created with consumer support in mind. Our customer care team is available seven days a week, staffed with a live team trained to help consumers navigate the CurrentC app, and any issues that might arise. The customer care staffers are prepared to help address consumer questions, providing honest, transparent answers.

Data Protection

As a part of the MCX network, merchants can connect directly and more efficiently with consumers. The current payments ecosystem frequently separates merchants from their customer

information and communication flow, allowing third parties to intercept and use that information for their own benefit. Our consumer-facing brand "CurrentC" puts control of that information back into the hands of consumers and merchants, allowing merchants to build engagement with their consumers directly around savings, loyalty and payments.

Consumer information is shared with a merchant only when a consumer chooses to interact with that merchant while using CurrentC. For example, if a consumer adds their "Merchant A" loyalty account, or pays with CurrentC at a "Merchant A" location, that information is only shared with "Merchant A". We do not share information about your relationship with "Merchant A" with any other merchant in our network. "Merchant A" may match that data (such as a loyalty account number) to info that already exists in their databases to personalize and improve that consumer's shopping experience. Consumer data is never sold.

Conclusion

We want to reiterate our appreciation for your interest in mobile payments technologies, and for providing Merchant Customer Exchange with the opportunity to share more about the innovation currently underway in the mobile payments space. We truly believe that mobile payments will provide a better opportunity for merchants and consumers to experience an improved shopping experience overall by:

- Providing consumers choice on how to pay
- Providing consumers flexibility on which handheld device they can choose
- Providing consumers loyalty, rewards, and savings benefits in a simple and easy "one-step" transaction

- Providing consumers with a more secure method of payment – by utilizing state of the art tokenization technology
- Providing merchants and consumers the ability to interact directly so that both parties have a more rewarding customer engagement
- Protecting customer data and merchant data so that third party providers are unable to target consumers or merchants without their knowledge

Mr. BURGESS. The Chair thanks the gentlelady.

Ms. Hughes, you are recognized for 5 minutes, please.

STATEMENT OF SARAH JANE HUGHES

Ms. HUGHES. Thank you, Mr. Chairman.

Mr. Chairman, Ranking Member Schakowsky, Representative Brooks from Indiana, and other honorable members of the subcommittee and committee who are present today, I am very pleased to be here with you to talk about mobile payments generally, and with the microphone, it will be even better—yes—and to talk about consumers in today's marketplace, and I am especially pleased not only to be here with you but to be here with my longtime professional acquaintance, John Muller of PayPal.

I have three disclaimers that are unique to me and a couple of others that relate to mobile that I think I should say. First, I am not here as a representative of Indiana University, so the trustees don't stand behind what I say. This is my personal opinion. I am also not here as a representative of the Uniform Law Commission, although I am currently working on a virtual currency project with them. And I am not here as a representative of the Federal Reserve System's Faster Payments Task Force, even though I am also working with them on that. So those are the formal usual disclaimers.

Now the personal ones. I do use PayPal, and I use PayPal on my phone. I do use Square, particularly to buy tickets and buy things, as Mr. Muller said, at farmers markets and at arts and crafts fairs and to make ticket purchases, and I use both Square and PayPal to make charitable contributions because it is not just the Christmas shopping season that we have right now; it is also the end-of-year charitable fund drive, and mobile payments are very important to charities. And as John segregated, even stationary e-commerce payments are very important to charities.

I don't use Apple Pay or Samsung, and the reason is because I don't have a new enough phone to make an Apple Pay, and I don't happen to be carrying Samsung.

So the committee asked us to look at four questions, and in the interest of time, the first was whether mobile payments were disrupting other forms of payments. And I personally believe the answer is not yet. And I am not certain when that moment will come when that will happen, but I think that it is a question of a level of adoption, and I am not positive, given that mobile payments will continue to rely on credit, debit, and other traditional sources of the funds for clearing and settlements, the degree to which mobile payments will disrupt in the way that we typically use the term. I would prefer to say that mobile payments can augment.

The second question the committee asked me to discuss was the security and what the technologies are. And while I agree that there have been some significant upturns in security, I like multifactor authorization, which we do not yet have with plastic cards in this country, but in other countries, we do. I like the tokenization options, and I like the geolocation options from a security perspective. I must be honest: from a privacy perspective, I don't like the geolocation option quite so much, but that is because

I am really a privacy hawk, and so I think that that is a significant issue.

The hurdles that are existing to widespread consumer adoption of mobile payments include something that MCX is going to solve by allowing ubiquitous types of utilities. But the other hurdle I believe requires significant consumer education expenses on the parts of the companies that are engaged in this, and I don't know whether you noticed, but yesterday, I saw an ad, I thought, for Samsung on this score. And I know that there have been others, but I think that there is an absence of consumer education which could be significantly enhancing the opportunities in this field.

Security depends in part on the contract between the user, me, and the providers. And so in addition to the Electronic Fund Transfer Act, which is older than my oldest child, who is 37, I think it also depends on the degree of supervision of payment processors who are not the providers and not chartered financial institutions to take good care of security in the middle.

And the next question that you asked involved privacy in this ecosystem. Many years ago now, by comparison, the privacy was put into place in the Gramm-Leach-Bliley bill, and the banks live with other privacy opportunities and responsibilities that they believe are considerable.

I would welcome any questions that the committee may have. Thank you.

[The prepared statement of Ms. Hughes follows:]



MAURER SCHOOL OF LAW
INDIANA UNIVERSITY
Bloomington

Prepared Statement of

Sarah Jane Hughes

Maurer School of Law, Indiana University

For the Hearing entitled

"The Disrupter Series: Mobile Payments"

Before the

Subcommittee on Commerce, Manufacturing, and Trade

Of the Committee on Energy and Commerce

House of Representatives

United States Congress

December 1, 2015

Mr. Chairman, Ranking Member Schakowsky, Representative Brooks from my home state of Indiana, and other honorable members of the Subcommittee, I am pleased to be invited to discuss mobile payments generally and the benefits and risks that mobile payments offer to merchants and consumers in today's marketplace. It appreciate the opportunity to be on this panel with distinguished representatives of U.S. Samsung Pay, the Merchant Customer Exchange, and my long-time professional acquaintance from the American Bar Association's Cyberspace Law Committee, John Muller of PayPal. This prepared statement and any remarks I may make during the hearing reflect only my personal views and do not necessarily reflect the views of the Trustees of Indiana University, or of the Uniform Law Commission, or of the Faster Payments Task Force operating under the auspices of the Federal Reserve Banks with which I am currently engaged in scholarly and public-service projects.

Mobile payments are among the most innovative and convenient payment options emerging across the world. They enable person-to-person payments globally using flip phones, text messaging and smart phones and in the U.S. are primarily used for person-to-business payments transactions using smart phones and other near-field communications systems. Among the many benefits that mobile payments offer in the U.S. and globally are their ability to provide unbanked and under-banked individuals and businesses to make payments more conveniently and at lower risk and cost than other payment options that maybe available.

Providers of mobile payments services vary significantly in size, the breadth and scale of the services they offer, and the extent of federal and state regulation in the United States that apply to their businesses generally. Their payment services in the United States are subject to differing supervision and consumer protection rules depending on whether the mobile payment device serves as an "access device" to the user's demand deposit account at a financial institution (the functional equivalent of a debit card) or the payment is billed to a wireless provider's monthly invoice to the user.

Mobile payments offer speedier conclusions to person-to-business payments in many cases than can be achieved through other payments options. As I noted when I testified before the Senate Committee on Banking, Housing and Urban Affairs in 2012, using a mobile payment to pay for a specialty coffee drink at Starbucks can be completed before the foam dissolves. This is particularly true because the mobile payment can be completed by the consumer even if the Internet connection the merchant has is offline; the wireless feature of mobile payments travels via the same wireless systems that operate the mobile phone or device.

Interest in speedier payments in the United States has been growing since my last testimony on mobile payments. This interest has prompted changes in the automated clearing house ("ACH") payments system operated under rules adopted by the National Automated Clearing House Association ("NACHA") and by the Clearing House Payments Company to speed up the clearing and settlement of ACH payments. Since 2013, the Federal Reserve Banks have been working on a project to create "faster payments" options for consumers and businesses and invited participants from many sectors to participate in its Faster Payments Task Force. The Task Force has been engaged in 2015 in efforts to frame the utilities, governance, legal structures and efficiency of faster payment solutions for domestic and cross-border transactions. I have been delighted to serve on the Faster Payments and Legal Working Groups created to support in this important effort.

Mobile payments can play important roles in raising individual contributions for disaster recovery, as they did for relief of victims of the Haiti earthquake, and for charitable and "crowdfunding" innovators and community and arts programming. It is conceivable – although I lack data to confirm this – that individuals who play in Daily Fantasy Sports also use mobile payments services and devices.

States and consortiums of state legislators and regulators including the Uniform Law Commission and the Conference of State Bank Supervisors have been watching mobile payments and

considering whether new state laws or regulations are needed to ensure the safe and transparent operation of mobile payments. The Uniform Law Commission, for example, sponsored a study committee on alternative and mobile payments in 2014; I served as the reporter to that study committee, which ultimately decided not to focus on mobile payments at that time. Since then, the ULC is re-considering whether to authorize a more in-depth study of mobile payments services that are not already regulated by state laws or federal legislation such as the Electronic Fund Transfers Act.

The balance of this prepared statement focuses on the issues on which the Chairman requested information and opinion. These are:

- How have mobile payment options disrupted the traditional payments landscape? What hurdles exist for widespread consumer adoption?
- What technologies have improved security for consumers' payment information in the mobile environment?
- What privacy considerations should be examined in the mobile payments ecosystem?
- How has mobile payment technology increased market access for the underbanked and small businesses?

I will respond to each of these questions in turn.

How have mobile payment options disrupted the traditional payments landscape? What hurdles exist for widespread consumer adoption?

The answer to this question is that it is difficult to tell the extent to which mobile payments options have disrupted traditional payments options. Despite the fact that two-third of American adults own smartphones, there is relatively little data about overall use of mobile payments by consumers in the United States. It appears that a much smaller subset of smartphone owners use them to make

mobile payments. One frequently cited reason is that U.S. consumers have numerous other convenient payments options, including credit and debit cards and assorted prepaid cards.

A recent survey of consumer users of new mobile payments options such as ApplePay, Samsung's Android payment product and others is only somewhat more encouraging. The survey executed by Trustev, a company that offers online fraud prevention services to retailers and banks, is described in an October 31, 2015 article in TECH INSIDER.[1] The author reported that:

> Trustev found that only about 1 in 5 people (20.7%) in the US who have an iPhone that works with Apple Pay — the iPhone 6 and newer — have even *tried* Apple Pay.
>
> Of those who have used Apple Pay, 56% report that they only use it once during a typical week, and 15.3% say they "never" use it during the week.
>
> The numbers are even lower for Samsung Pay and Android Pay. (Although the two services are different, Trustev combined them for the survey because Samsung Pay is only available on a small number of Android devices.)
>
> Only 14% of people who have the Samsung Galaxy S5 and S6 have ever used Samsung Pay or Android Pay, according to Trustev. Of those people who have, only 36.17% use it once in the typical week and 38.3% report they "never" use it.
>
> Rurik Bradbury, the chief marketing officer of Trustev, told Tech Insider that he thinks mobile payments haven't caught on because paying with a credit card isn't that difficult.
>
> "It just seems to me that there's not much of a problem Apple Pay fixes," Bradbury said. "Paying with a credit card is very easy. It's a habit everyone has."
>
> Indeed, Trustev also found that more than 82% of survey respondents reported that paying with a credit card in a store is "very easy" or "easy."[2]

The article points out that these products are new. Apple Pay was introduced in September 2014 and the Samsung and Android mobile payments options were introdcued in 2015, with the Samsung product introduced only a month before the survey and Adroid Pay on September 11, 2015.[3]

---

[1] Tim Stenovic, *A new survey shows people aren't really using Apple Pay,* TECH INSIDER (Oct. 31, 2015), http://www.techinsider.io/not-very-many-people-use-mobile-payments-2015-10. The survey included 1,000 respondents who had iPhones and Apple Pay and 1,000 respondents using Samsung Galaxy or other Android smart phones. *Id.*

[2] *Id.*

Other studies suggest a broader use of and satisfaction with mobile payments options. The same article in TECH INSIDER reported:

> Surveys by the Auriemma Consulting Group this year consistently found that 42% of iPhone 6 and 6 Plus owners have used Apple Pay, and that people who use the feature are very satisfied with it.
>
> When reached for comment, a Samsung spokesperson said that when the company beta-tested Samsung Pay in the US, 90% of people who used it said they were most likely to continue using the feature, and 90% reported they were most likely to recommend it to a colleague or friend.
>
> Samsung also said on Wednesday that people in the US who use Samsung Pay are likely to use it again — the company reported an average of eight Samsung Pay transactions per user.[4]

These surveys leave me with a more optimistic impression about future usage of newer mobile payments products, including Apple Pay, Samsung and Android Pay. These are early days, particularly for Samsung and Android Pay. Investors interested in mobile payments technologies should not depart this space based on such early returns, in my opinion. With three new major-branded mobile payments offerings in the past 15 months, it simply may be too soon to tell the extent to which how consumers will adopt which of these mobile options or others that may be available.

The logical, follow-on question to this first question is whether there are hurdles to consumer adoptions of mobile payments products? The answer in my opinion is that there are no legal barriers to broader adoption. But that there may be knowledge barriers to adoption—that is, that consumers do not adopt new payments technologies until they understand how they work, who backs the payment product, and what to do if the consumer has a complaint about the provider's performance or the performance of the merchant that accepted payment via the mobile option. In other words, I am inclined to think that additional consumer education about these products could make consumers more

---

[3] *Id.*
[4] *Id.*

likely to use them if they had smartphones capable of supporting these new options. This would require work by mobile payments providers to make their products and dispute-resolution procedures as transparent and efficient as possible. This need for information and product differentiation is also present in other emerging payments options being offered in the United States.

I might cite one barrier to greater use of mobile payments that comes from the merchant side – the cost of and training associated with acquiring new "readers" to receive information for contactless payments, etc. I do not have data on how much it costs merchants to acquire a contactless reader or how much training and monitoring of employees it takes to get to smooth and sufficiently speedy use of one to make it worthwhile for merchants. Ms. Deckinger, however, may be able to speak to this issue. But I do recall that costs that merchants had to incur to get early-stage smart-card payments devices from 1995 through to the end of the Mondex and Citi experiments in this country were cited as a reason why the smart-card option was so hard to grow.

What technologies have improved security for consumers' payment information in the mobile environment?

Among the most-cited perceived impediments to wider consumer adoption of mobile payments options is security. I suspect that the data-security breach episodes by major retailers over the past decade have made consumers increasingly concerned about data security, just as they have driven U.S. merchants and financial services providers to increase their attention to ensuring effective security.

Among the most important improvements in the mobile payment ecosystem are the availability of new security features on the phone physically, such as passwords or passcodes set by users, fingerprint-reading functions, and the ability to delete data remotely in the event that the phone is lost or stolen. Multifactor authentication and tokenization are additional options for greater mobile payments security. Multifactor authentication effectively requires the username, password or passcode

(including a fingerprint), and the device or phone itself. The phone's location function allows the authentication process to verify that the phone and consumer are in the same location. This verifies the payment from the outset, but it may not prevent loss of the payment or user data downstream as the payment "instruction" moves towards clearing and settlement. Multifactor authentication also is not used in connection with other features, such as reward programs and customer-relationship management or with remote (device not present) transactions.

The tokenization option of enhancing security permits strong security along the downstream route to clearing and settlement, in rewards programs and in customer-relationship management. Tokenization works only for one-time verification; it prevents linkage of a payment to prior payments by the user or the user's phone or device.

Apart from technological security aids, providers of mobile payments services face federal and state compliance obligations that may encourage them to enhance the security of their systems. The Federal Trade Commission's "Safeguards" Rule, codified at 16 C.F.R. Part 314, mentioned in the Majority Memorandum for this hearing, covers mobile payments providers and downstream processing, clearing and settlement services connected to them. Additionally, the Majority Memorandum noted, the FTC can use its FTC Act Section 5 authority to secure remedies for violations by mobile payments providers that are not banks or communications carriers themselves. However, the recent FTC Administrative Law Judge decision in In the Matter of LabMD, Inc.,[5] Initial Decision (Nov. 13, 2015), casts doubt on the use of Section 5's "unfair and deceptive acts or practices in commerce" authority as a means of redressing

[5] FTC Docket No. 9357. The original administrative complaint was filed on August 28, 2013.

security breaches unless the FTC staff can prove more than theoretical harm to consumers as a result of the breach.[6] The FTC Complaint Counsel filed a Notice of Appeal on November 24, 2015.

As the Majority also noted, about a quarter of the States include financial account, credit and debit card information under their statutory definitions of "personal information." Private actions brought for violations of these State statutory requirements also have encountered problems proving injury to consumers in some courts.

Mobile payments providers and those seeking to enter this ecosystem as providers or processors nevertheless can follow some "best practices" for securing data required to receive, clear and settle payments. I would encourage merchants and others engaged in receipt or processing of mobile payments to use the recent FTC guidance on simple security practices, *Start with Security: A Guide for Business.* [7] The Guide sets forth a ten-step outline of what business can do to enhance the security of customers' information, both personal and financial.

Efforts by federal and state bank regulators also promise to yield stronger security ecosystems for all payments providers. In this connection, I would cite the work by the FFEIC in 2015 on its new Cybersecurity Assessment Tool, led by Valerie Abend of the Office of the Comptroller of the Currency, and the stronger cybersecurity requirements expected from the New York State Department of Financial Institutions, spearheaded by the former Superintendent Benjamin Lawsky. Although the Cybersecurity Assessment Tool and the New York DFS requirements may not affect every provider directly, efforts such as these offer encouragement and guidance options to providers beyond those directly affected.

What privacy consideration should be examined in the mobile payments ecosystem?

[6] Fed. Trade Comm'n., Press Release, *Administrative Law Judge Dismisses FTC Data Security Complaint Against Medical Testing Laboratory LabMD, Inc.* (Nov. 19, 2015), https://www.ftc.gov/news-events/press-releases/2015/11/administrative-law-judge-dismisses-ftc-data-security-complaint.

[7] (Sept. 2015) https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

In my 2012 Senate testimony, I noted that harvesting consumer information from mobile payments transactions places more personally identifiable information and more personal financial information in the hands of merchants and the downstream payment system participants including non-bank payments processors. I have found little evidence of change on this front since July 2012.

Many non-bank payments processors are not regulated by the States or federal regulators to the same degree that depository institutions such as commercial banks and credit unions, or providers operating under State "money transmitter" licenses, such as PayPal, are. However, the 2000 Federal Trade Commission rule implementing Title V (Privacy), Subchapter I of the Gramm-Leach-Bliley Financial Services Modernization Act of 1999, codified at 15 U.S.C. 6801-6809, covers all participants in the provision of consumer financial products and services. 65 Fed. Reg. 33645, 33655, 33655 (explaining the inclusion in the final "Privacy" rule's definition of "financial institution", 16 C.F.R. § 313.2(k), entities engaged in providing data processing and data transmission services in connection with financial products and services provided to consumers, citing Section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. § 1843(k)). The "Privacy" regulations promulgated by other federal financial regulators have similar but not identical coverage. Thus, between the rule written by the FTC in 2000 and now also enforced by the Consumer Financial Protection Bureau, and the rules written by the Comptroller of the Currency, Federal Deposit Insurance Corporation, and Board of Governors of the Federal Reserve System, most of the providers of mobile payments should have a sufficient roadmap on how to handle the personal identifiable information and financial information that they obtain from the processing of payments via mobile devices.

The Committee may be aware that commercial banks have expressed concerns about privacy and security in non-bank payments processing in the past.[8] The potential for a mobile payment provider and the downstream payments participants necessary for clearing and settlement of the payment back to the merchant involved to collect and use information about the customer's spending habits and vendors of choice is and will continue to be substantial. Whenever additional entities handle payment and user information, the risks of capture and improper uses of these data grow. Thus, a multi-party mobile payments downstream network and could create privacy risks in a degree comparable or greater than privacy risks experienced in credit and debit transactions – unless all participants commit to privacy standards and comply with any applicable limitations on re-use and implement and monitor their systems for interceptions by intruders.

It is not clear to me that Congress should enact or require agencies to promulgate additional compliance obligations on merchants or mobile payments providers to ensure privacy at this time. But, I think it is far to point out that consumers will forego payments providers and merchants who do not protect their privacy or guard the systems that process, clearing and settle payments to a sufficient extent. We only have to look at the downturn in business for merchants that suffered data-security breaches over the past few years to observe how quickly consumers can take their business to a different merchant, or in the case of mobile payments usage, to "hang up" on mobile payments in favor of another payment option.

How has mobile payment technology increased market access for underbanked consumers and small businesses?

The success of mobile payments outside the United States, particularly among unbanked and underbanked individuals and businesses in Africa, suggests that mobile payments can benefit

[8] *See, e.g.*, Statement for the Record from Robert C. Hunter, Deputy General Counsel, The Clearing House Association, L.L.C., to The Subcommittee on Financial Institutions and Consumer Credit of the House Committee on Financial Services, June 29, 2012.

underbanked persons greatly. In this country, we are seeing the emergence of smartphones as the key connectivity option for less affluent persons and for those who reside and work in rural areas or parts of cities where fewer bank branches operate than they formerly did. Wireless phones have replaced land lines in these populations and also provide their Internet connections. Mobile payments offer attractive options for making payments on a person-to-person ("P2P") or person-to-business ("P2B") basis for those businesses that can accept payments via a mobile option.

Media coverage suggests that home-maintenance and garden-care businesses, house-cleaning services, plumbers, and massage therapists and many more types of small businesses use mobile payments as a preferred payment option. (They also may deposit checks they receive via remote-deposit options on smartphones offered by an increasing number of depository institutions.) These businesses may receive larger-dollar payments via mobile services than those in some retail businesses, but, regardless of the dollar values being paid, using mobile payments can help small businesses grow their revenues and profitability. They offer special opportunities to build customer loyalty through rewards programs and geo-locationally based or directed advertising that some consumers enjoy.

The convenience for small businesses of using mobile payments can be significant. The business owner does not have to worry about keeping track of payments in cash or check, does not have to add trips to make deposits to their daily or weekly scheduled, and has a reliable report of receipts and deposits from the mobile or remote-deposit provider. As I mentioned in my 2012 testimony, taking mobile payments may help businesses of every size deter fraudulent charges at the point of sale – even as credit cards with chips become common in the United States – because of the dynamic credentialing that mobile payments options provide via location information and unique identifiers for each transaction. Square and Apple Pay offer even more unique credentialing options in the forms of matching the face of the consumer making the payment and the photo stored with Square or the fingerprint identifier used by Apple Pay.

Another group of "small businesses" that benefit from mobile payments in the U.S. are farmers and local operators of farm markets, artisans who sell at arts fairs, and small arts organizations. I serve on the board of The Yard, Inc. , a dance colony in Massachusetts, that began using Square for ticket sales and credit-and-debit contributions about four years ago. The convenience for The Yard and for our patrons has been a boon to our earned income and personal contributions, and the manner in which we can use this excellent option also saves us accounting and processing costs that really adds value to The Yard's bottom line.

From the perspective of consumers, mobile payments options offer more secure payments alternatives than cash and lower-cost and more secure means of making payments than postal money orders or commercial money orders. They also enable payments by holders of prepaid cards and payroll cards remotely, which saves time and transportation costs. Thus, market access has already increased for the unbanked and underbanked, but I have found no firm evidence of the current uses of mobile payments among these two traditionally underserved groups. I would expect that as providers such as Apple, Samsung, and Android and others expand their offerings that these groups will benefit further from the use of mobile payments and that the businesses with whom they deal will benefit as well.

Thank you, Mr. Chairman and Representative Schakowsky, for the opportunity to appear before you this morning. I would be pleased to answer questions you may have.

Mr. BURGESS. The Chair thanks the gentlelady.
Mr. Ahn, you are recognized for 5 minutes, please.

STATEMENT OF SANG W. AHN

Mr. AHN. Chairman Burgess, Ranking Member Schakowsky, and distinguished members of the subcommittee, thank you for the opportunity to testify on behalf of Samsung Electronics America. For today's hearing, I would like to introduce you to Samsung Pay, which combines security, simplicity, and widespread acceptance like no other mobile payment solution. Whether it is fighting fraud or helping consumers zip through Black Friday checkout lines, Samsung Pay benefits consumers, retail merchants, and financial institutions.

For consumers, Samsung Pay is accepted virtually anywhere you can swipe or tap a card. It is secure, easy to use, and simple. Swipe up—I will demonstrate on my phone. Swipe up to launch the application. Confirm your identity with a fingerprint. Hover the device over the payment terminal and pay. It is that simple and has the widest acceptance of any mobile payment service.

For merchants, Samsung Pay helps merchants provide a secure, innovative, and fast payment experience. Samsung Pay supports all payment terminal types, including magnetic stripe, NFC, and EMV terminals. For financial institutions, Samsung Pay has security features, including tokenization and fingerprint authentication, that limit fraud and reduce liability. So those are Samsung Pay's benefits in broad strokes.

Importantly, our innovation was made possible by the Government's decision to have consumers pick the winners in the mobile payments space without additional regulations. Going forward, Congress should continue to allow consumer choice to drive innovation and differentiation in this space.

Before diving further into Samsung Pay, it might help if I highlighted Samsung's presence in America and how our U.S. employees are contributing to Samsung Pay. Headquartered in New Jersey and with facilities in Dallas, Palo Alto, Austin, South Carolina, New York, and Massachusetts, Samsung Electronics America is a recognized innovation leader in smartphones, consumer electronics, IT, and home appliances. We employ approximately 15,000 people in America, and our $15 billion investment in our Austin semiconductor plant is the largest single site foreign direct investment in America. In regard to Samsung Pay, our U.S. employees have driven much of Samsung Pay's development and success.

Several years ago, Samsung Pay's R&D teams examined mobile payments. We found that consumers would transition from plastic cards to mobile payments if the technology solution is, one, secure; two, simple to use; and, three, widely accepted at most merchants nationwide. We concluded that many companies can make a secure and easy-to-use mobile payment solution, but the trick is making the payment solution widely accepted by merchants. Current solutions rely on NFC, near field communications. Although NFC shows great promise, only a small fraction of merchants in the United States have adopted NFC-equipped point-of-sale terminals. Without the infrastructure in place for accepting NFC-based trans-

actions, consumer acceptance of NFC-only mobile payment services has remained low.

Enter Samsung Pay. Unlike other mobile wallets in the market, Samsung Pay lets you pay at most any terminal where you can swipe a credit card. To accomplish this, we are using an innovative new technology known as MST, magnetic secure transmission. MST leverages magnetic stripe technology already accepted by more than 30 million merchants around the world. Specifically, MST emulates a swipe transaction thanks to a tiny coil in our phones that transmits the same magnetic data and code that magnetic stripe readers normally get from a credit card or debit card. By including both MST and NFC technologies in our phones, Samsung Pay enables customers to make secure payments almost anywhere regardless of the merchant's point-of-sale equipment.

Because of Samsung Pay's wide merchant acceptance, we can make a meaningful contribution to payment security by enabling the largest footprint of secure, tokenized payments. With tokenization, Samsung Pay never provides a consumer's personal account number to a merchant. Instead, Samsung Pay provides merchants with tokens yielded created by the consumer's credit card company that enable the merchant to process the transaction without exposing sensitive customer information to potential data thieves.

Samsung Pay utilizes biometrics as well, which allows users to apply a fingerprint to the phone's built-in sensor to authenticate a transaction. Additionally, our smartphones incorporate the Samsung KNOX security platform, keeping all payment data locked and secure.

Finally, getting user privacy right is critical. For Samsung Pay, we do not and cannot monitor user purchases. The transitional details areencrypted and can only be decrypted on a consumer's device.

Samsung wants all consumers, regardless of income, to make secure payments. No other mobile manufacturer reaches as diverse an audience as Samsung or offers its consumers such a wide array of innovative products at different price points. Accordingly, we closely are examining how to include Samsung Pay in a greater range of devices. As we do so, we would welcome your thoughts any input from your constituents.

Thank you, again, for holding this hearing and allowing Samsung to share our thoughts and benefits about mobile payments.

[The prepared statement of Mr. Ahn follows:]

SAMSUNG

PREPARED STATEMENT OF SAMSUNG ELECTRONICS AMERICA

For the

COMMITTEE ON ENERGY AND COMMERCE OF THE U.S. HOUSE OF REPRESENTATIVES SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

On

THE DISRUPTER SERIES:

MOBILE PAYMENTS

Sang W. Ahn
Chief Commercial Officer, U.S. Samsung Pay
Samsung Electronics America
December 1, 2015

Prepared Statement of Sang W. Ahn

Chairman Burgess, Ranking Member Schakowsky, and distinguished members of the Subcommittee, thank you for the opportunity to testify on behalf of Samsung Electronics America. For today's hearing, I'd like to introduce you to Samsung Pay, which combines security, simplicity, and widespread acceptance like no other mobile payment solution. Whether it's fighting fraud or helping consumers zip through Black Friday checkout lines, Samsung Pay benefits consumers, retail merchants, and financial institutions.

Consumers. Samsung Pay is accepted virtually anywhere you can swipe or tap your card: from the grocery store to the coffee shop to your favorite department store. It's secure, easy to set up, and simple to use. Swipe up to launch the app. Confirm your identify with your fingerprint. Hover your device over the merchant's payment terminal to pay. Done – with by far the widest acceptance of any mobile payment service.

Merchants. Samsung Pay also increases security for merchants and keeps their customers happy by providing a safe and innovative payment experience. It does this by leveraging existing infrastructure

and supporting all payment terminal types, including magnetic stripe, NFC, and EMV terminals. This means merchants do not have to upgrade or buy additional equipment to support competing mobile wallets. It also increases checkout speed – the consumer just taps their phone to the merchant's PoS terminal, and that's it.

Financial Institutions. For banks and other financial institutions, Samsung Pay's tokenization and fingerprint authentication features limit fraud and reduce liability. Our solution also integrates cleanly with the ecosystem's existing and planned investments in security.

So those are Samsung Pay's benefits in broad strokes. Importantly, our innovation was made possible by the government's decision to have consumers pick the winners in the mobile payments space and to refrain from adopting mobile payment-specific laws and regulations. Going forward, Congress should continue to allow consumer choice to drive innovation and differentiation in this space.

I. BACKGROUND ON SAMSUNG ELECTRONICS AMERICA

Before diving further into Samsung Pay, it might help if I highlighted Samsung's presence in America and how our U.S. employees are driving Samsung Pay's evolution.

Headquartered in New Jersey, and with major facilities in Dallas, Palo Alto, Austin, South Carolina, New York, and Massachusetts, Samsung Electronics America is a recognized innovation leader in smartphones, consumer electronics, IT, and home appliance products. We employ approximately 15,000 people in America, and our $15 billion dollar investment in our Austin Semiconductor plant is the largest single-site foreign direct investment in America. Additionally, in the past year, our parent company, Samsung Electronics Corporation, moved Samsung's Global Centers for Excellence in services and content and marketing to California and New York. And our employees at those two locations – California and New York – have driven much of Samsung Pay's development and success.

II. SAMSUNG PAY – BRINGING SECURE MOBILE PAYMENTS TO CONSUMERS

Several years ago, Samsung's R&D teams began plans to extend our ingenuity into mobile payments. Based on our research, we found that consumers would only transition from plastic cards to mobile payments if the technology solution is: (1) secure; (2) easy to use; and (3) widely accepted at merchants nationwide. We concluded that many of the world's top tech companies could make a secure and easy to use mobile payment solution. The tricky part – and what held back the widespread consumer adoption of mobile payments – has been the reliance of other mobile payment solutions on NFC (Near Field Communication) technology.

Although NFC technology shows great promise for future mobile payment solutions, only a small fraction of total merchants have adopted NFC-equipped PoS terminals. Without the infrastructure in place for accepting NFC-based transactions, consumer acceptance of NFC-only mobile payment services has remained low.

Enter Samsung Pay. Unlike other mobile wallets in the market, Samsung Pay lets you pay at most any terminal where you can swipe a credit card. To accomplish this, we're using an innovative new technology known as MST (Magnetic Secure Transmission). MST builds on the magnetic stripe payment terminal technology already accepted by more than 30 million merchants worldwide. Specifically, MST emulates a swipe transaction thanks to a tiny coil in our phones that transmits the same magnetic code that magnetic stripe readers normally get from a credit or debit card. By including both MST and NFC technologies in our phones, Samsung Pay enables customers to make secure payments at almost any merchant, regardless of the merchant's PoS equipment. EMV, NFC, traditional magnetic stripe terminals . . . SamsungPay works virtually everywhere.

Samsung is also building an extensive ecosystem to broaden acceptance of Samsung Pay. In America, we're partnering with leading financial institutions such as American Express, MasterCard, Visa and Discover, major banks including Bank of America, Chase, Citi, Suntrust,

U.S. Bank, and additional ecosystem partners including First Data, Synchrony Financial and TSYS.

III. SAMSUNG PAY = UBIQUITOUS SECURITY, NOW

Simply put, Samsung Pay has revolutionized payment security for consumers. Samsung-Pay users can now make secure, tokenized payments virtually anyplace that accepts a credit or debit card. No other payment solution comes close.

With tokenization, Samsung Pay never provides a consumer's 16 digit Personal Account Number (PAN) to a merchant to process a transaction. Instead, Samsung Pay provides merchants with one-time tokens – created by the consumer's credit card company (e.g., Visa, Mastercard, AmEx) – that enable the merchant to process the transaction without exposing sensitive customer information to potential data thieves.

Samsung Pay utilizes biometrics as well, which allows users to apply a fingerprint to the phone's built-in sensor to authenticate a transaction. Additionally, our smartphones incorporate the Samsung KNOX security platform, keeping all payment data locked and secure.

Certainly, other mobile payment solutions employ tokenized transactions. But, as I mentioned earlier, these solutions only work in the small fraction of stores with NFC-equipped terminals. Samsung Pay enables consumers to make secure transactions almost anywhere.

Finally, any mention of security is not complete without a discussion of user privacy. At Samsung, we take customer privacy very seriously and have embedded privacy controls in the Samsung Pay platform.

For example, Samsung does not – and cannot – monitor user purchases. After a payment is accepted by the issuing bank, the card network may optionally send a notification back to the device that contains details of the accepted transaction. But these details are encrypted, and can only be decrypted on the consumer's device.

IV. What's next?

Samsung wants to enable all consumers – regardless of income, ethnicity, and technological sophistication – to make secure payments. Financial inclusion is something Samsung takes seriously given our unique position as a leading provider of phones to lower-income

individuals and the broader underbanked community. Simply no other tech company reaches as diverse an audience as Samsung, and no other company offers consumers such a wide-array of innovative products at different price points. Accordingly, we're closely examining the opportunity to include Samsung Pay in the greatest range of devices for 2016 and beyond. As we do so, we'd welcome your thoughts and any input from your constituents.

* * *

Thank you again for holding this hearing and for allowing Samsung to share our thoughts on the wide-ranging benefits of mobile payments.

Mr. BURGESS. The Chair thanks the gentleman.

The Chair thanks all of our witnesses for providing testimony today and food for thought.

We will move into now the Member question part of the hearing. I will begin recognizing myself for 5 minutes for questions.

Ms. Deckinger, let me just ask you, obviously, we have heard from Mr. Ahn about some things that are rather device-specific, but you talk about being agnostic as to the type of device. So how does that interplay into the consumer experience having a device, any device, which is then able to use your product?

Ms. DECKINGER. Thank you so much for your question. We are very focused at MCX on creating consumer choice and enhancing that, making it available to all consumers. We feel like it is very important to have consumers have the option to use whatever device they would like to. Therefore, we have designed our technology to work on all devices, all smartphones. Virtually any smartphone that a consumer has can leverage our technology pretty easily.

Mr. BURGESS. I have got to ask the question. What about a flip phone? Some of us still have them.

Ms. DECKINGER. We are not quite there yet.

Mr. BURGESS. Not quite there yet. Mr. Ahn, you bring up some great points, and I think you heard Ranking Member Pallone talk about providing services to the unbanked in places where the infrastructure for check to bank does not exist, whether it be because of civil strife or warfare or poverty. So you actually could to some degree bridge that gap, could you not, with the devices that you are talking about?

Mr. AHN. That is right. We have the opportunity through our phone ecosystem—and remember we have over 700 million devices in market around the world, and we are a global company—we have the opportunity through application to provide payment solutions that are relevant for consumers. What we are doing in the United States with our recent launch of Samsung Pay is providing an opportunity for the user, the consumer, to pay at any merchant location, whether it is a big box retailer, like many of the MCX merchants, or small mom-and-pop shops.

MCX, as you remember, there are many partners within MCX that we are very close with; we are in discussions as partners. MCX is designed to be a large consortia of the largest merchants, and they are relevant and important from a consumer experience point of view. However, we think that we need to go beyond just large box retailers into mom-and-pop stores. Anywhere there is a transaction, we want to be there for the consumer. So that is our near-term opportunity.

Having said that, I think it is the early stages of this payment ecosystem, and all innovations are helpful. As a rising tide lifts all boats, we want all innovations to succeed and move the payment ecosystem forward, primarily creating additional security for the user moving forward.

Mr. BURGESS. Very good. Mr. Muller, let me just ask you, PayPal, one of the originals and I think when I ran my first campaign 13 or 14 years ago, I actually had a PayPal option as far as for people who wanted to support. You have probably had more experience in this space than almost anyone else. How do you lever-

age the security? How do you add layers of security to or additional layers of security for the transactions for the consumers?

Mr. MULLER. So it is always a matter of trying to add security with user convenience and the user experience, and that is what the mobile device offers in a somewhat unique way, is the way to improve both the user experience and security, and that is a rare thing in the payments field, through the kinds of technologies we have already mentioned, like the device location or unique device identifier, and do it in a way where the user controls what information they are sharing. So that is the Holy Grail we are all trying to achieve. And I also want to emphasize that all the same risk programs are still running in the background, so we don't assume that there is a silver bullet type solution in security. So even if we do have a customer who is taking advantage, say, of the fingerprint authentication or device location and they pass that test, we are still running all these other tests in the background looking for risk variables in the transaction. So it is a matter of adding to risk-reducing programs that already exist, not substituting them purely with new types of authentication or security.

Mr. BURGESS. Well, thank you. This is not a question. It is an observation. We had a hearing here not too terribly long ago about senior citizens who were taken advantage of by various phone solicitations. And as this technology becomes easier and more ingrained, I would just ask you to be thinking about, you have always got to stay one step ahead of the very clever thief out there, so to help protect senior citizens against this type of activity, do be thinking about what type of safeguards may be incorporated into the technology.

With that, I am going to recognize Ms. Schakowsky for 5 minutes for questions.

Ms. SCHAKOWSKY. So, Ms. Deckinger, we celebrated Small Business Saturday. I went to a number of small businesses, took selfies, in my neighborhood. So your technology right now really favors larger operations. Right?

Ms. DECKINGER. At the moment, yes. We are in the early stages of a pilot at the moment. So we are still developing our technology and working to build a network that consumers can use CurrentC in places where they shop every day, yes.

Ms. SCHAKOWSKY. I wanted to ask some questions about consumer privacy.

Professor Hughes, what kind of data is collected by these apps, and is that data different from what a more traditional means of payment might collect, like a credit card?

Ms. HUGHES. Thank you, Ms. Schakowsky. I think it depends a great deal on the system. Mr. Ahn has just said that Samsung Pay which was relatively recently introduced in the United States, does not have, does not allow the merchant to see any of the information, and so the authentication device does not share that information with the merchant. It operates in a more traditional way, like an escrow service, if I understood you correctly, for that information. You keep it, and you are passing the payment through, but you are not passing the consumer's information through. PayPal——

Ms. SCHAKOWSKY. Is that a correct description?

Mr. AHN. That is correct. The way we implement today is we send a data package over that is completelyencrypted, and no one sees what is inside.

Ms. SCHAKOWSKY. Is that unique to your company?

Mr. AHN. No, it is not.

Ms. SCHAKOWSKY. But it is not mandated in any way right now. Right?

Mr. AHN. This is one implementation of tokenization that is prevalent in the market by leading technology companies.

Ms. SCHAKOWSKY. OK. Go ahead.

Ms. HUGHES. I was about to say, but I think your clarification was extremely helpful, that PayPal also operates in an escrow mode because the transaction flows into PayPal, and then PayPal processes the payment transaction in a way that is lots more like an escrow than many people believe. That is not true of every app that might be available, which is one of the reasons why I said when it comes to security and, indeed, to privacy also, it really depends on who the provider is, whether it is a branded company like PayPal and Samsung, whether it is an app for another purpose.

The manner in which tokenization is employed is also very random at this stage, so there are a number of alternatives that do not have the same levels of security and/or customer privacy as Samsung and PayPal have.

Ms. SCHAKOWSKY. You know, my experience with these kinds of things is that they ask you to accept the deal. And that is preceded by a lot of stuff on a very small device that you have to figure out in legalese whether or not you push accept. I would challenge almost anyone whether or not they carefully scrutinize those things before pushing "I accept" and then moving on to use. I am just wondering if since there are alternatives, some more secure than others, should there be some standardization? Should there be some requirements to protect consumer privacy?

Ms. HUGHES. I had mentioned earlier that I am a privacy hawk, but I believe very firmly that everybody should have the privacy protections that Congress and many States have already provided, basically Congress has provided. I believe that everybody should have the same access to those privacy protections, but I also believe that one of the dynamic forces in mobile payments is the ability to compete to provide better than other people do. So the companies that are working with multifactor authentication, working with tokenization, that are doing, as Mr. Muller suggested, continuing to run their risk platforms, which are old-fashioned, artificial intelligence operations in the background that are monitoring the payments transactions that are coming through their systems. As long as there is a floor, then I believe people should be able to compete to offer better tokenization, more extensive or unique——

Ms. SCHAKOWSKY. That is something we are going to have to consider if we think competition based on level of risk and protection for consumers is a legitimate way to compete.

I have actually run out of time, so I am going to I yield back.

Ms. HUGHES. Would you like me to answer the question?

Ms. SCHAKOWSKY. Yes, sure.

Ms. HUGHES. I think the answer is right now among the various payment systems in the United States, there is already a broad

array of risk that relates to privacy and security. And because we have silos around different kinds of payments, this has been the constant in the marketplace back to the 1970s or the early 1960s. And efforts to harmonize that were not successful in the past, and whether they can be successful in the future remains to be seen.

Ms. SCHAKOWSKY. Can I just say, I am not talking about necessarily harmonizing the method or the technology, but I am talking about setting a level of risk that is acceptable in the marketplace. So I need to move on.

Mr. BURGESS. The Chair thanks the gentlelady.

The Chair recognizes the vice chair of the full committee, Mrs. Blackburn, for 5 minutes for questions, please.

Mrs. BLACKBURN. Thank you, Mr. Chairman.

Ms. Schakowsky might be moving on, but I will just kind of put a comment to the end of her words. We have had a privacy and data security working group here at Energy and Commerce, and we all are focused on making certain that consumers are safe in the marketplace. And Mr. Welch and I have worked on a data security bill. And we continue to try to push this forward so that we can do some preemption, establish some breach notification, and bring some certainty to bear. So I appreciate the questions that are being asked around this issue this morning, and we hope that you appreciate them too.

Ms. Deckinger, I want to come to you. Those of us who appreciate the virtual marketplace and want to see people in it, and then we see articles like this, and it makes you go "ouch." It is the "Apple Pay Rival and Walmart-Backed MCX Hacked, User Emails Snatched." And this was in your beta test period. It was October 2014. That was a Forbes article that was written about this.

And, Mr. Chairman, I am going to pass this down so Ms. Schakowsky can see it because I know she is, like me on this privacy issue, very concerned about that.

I want you to provide some information about that hack and what you did on resolving it.

Ms. DECKINGER. Yes. Thank you so much for the question. So a subcontractor of MCX, not MCX itself, had a security incident where some emails were released. That subcontractor was immediately terminated as a partner.

Mrs. BLACKBURN. How long did it take you to isolate the hack?

Ms. DECKINGER. Immediately. We also opted to notify folks within hours of finding out, very rapidly after finding out that this occurred, and we have taken extensive precautions. Security is very important to us. Obviously, it is very important to our users. We have taken extraordinary precautions now to address any issues that we found with that subcontractor with additional subcontractors that we have then partnered with in the future. We continue to evolve our security platform and are always looking. There are always, as someone mentioned earlier, clever and creative criminals out there who will seek to look for data, and no security is perfect. But we are working hard to achieve a——

Mrs. BLACKBURN. OK. Let me pick up on that evolution in this process. Talk to me about what precautions you are taking around data security when it comes to the multifactor authentication or tokenization. What are you moving toward, and are you pleased

with those advances? And I am coming to each one of the rest of you on this panel, so get ready. The clock is ticking, 30 seconds.

Ms. DECKINGER. So we have a cross-functional security council internally within MCX. We work together regularly and meet regularly to discuss the latest technology innovations, the latest security innovations. We are always evaluating what is possible to make things more secure for consumers, to make them more secure for merchants and for the app. We are always—always—implementing the state-of-the-art technology that we can, whatever is available for us to implement, and we will continue to do so. Obviously, the trust of consumers and their feeling of security when using an app is of the utmost importance, and we recognize that, and so we have worked to make sure that we are always sitting on the cutting edge.

Mrs. BLACKBURN. OK.

Mr. Muller?

Mr. MULLER. OK. I think for all of us, you will probably hear the theme that it is constant battle and constant investment in security because the fraudsters are out there also continually changing their methods of attack. And so we have tried to make that investment, and it is certainly a huge part of our cost base. And then we also try to do what we can, first of all, to minimize data collection, because, frankly, if we don't have the data, then even if we were somehow to be breached, it would be less vulnerable.

Mrs. BLACKBURN. OK. Mr. Ahn, I am going to come to you. Talk about the Fast Identity Online Alliance and your protections.

Mr. AHN. So the security protocols we put in place are quite extensive. What we think about is putting multiple walls up such as the fraudsters have to hop over many, many steps to reach the information. One of the things that we do is we have at the integrated chip level, the microprocesser alone has a way for us through KNOX, which is our proprietary solution, to shut down in the event of a rooting event. The application must be authenticated by fingerprint or PIN to get into the application. If the phone is lost or stolen, we have the ability to remotely turn off payment credentials completely and turn them back on. And when the card networks——

Mrs. BLACKBURN. So hold on. So you have got three tiers of encryption before you get to——

Mr. AHN. We have multiple ways of protecting the consumer information. The last one is that the card networks and credit card companies that we work with themselves have the ability to remotely turn on and off tokens. So what happens—and the last and most important piece is we purposely architected our solution to not store personal information and card transaction information. We only pass along a token. And so, for us, there is no central point to hack. The only information that is available temporarily is transaction history for the last 10 transactions on your device, and this one device is not a rich enough target for fraudsters. So that is how we view security.

Mrs. BLACKBURN. Thank you.

I yield back.

Mr. BURGESS. The Chair thanks the gentlelady.

The Chair recognizes the gentleman from New Jersey, Mr. Pallone, ranking member of the full committee, 5 minutes for questions.

Mr. PALLONE. Thank you, Mr. Chairman.

I wanted to ask Professor Hughes, a consumer's ability to dispute unauthorized charges on a mobile payment varies depending on the payment method being used. For example, a consumer's liability for unauthorized charges on a credit card after a certain date is lower than on a debit card. Could you tell me what protections are available to consumers who do not have access to a credit or debit card and choose to link a mobile payment to their mobile phone bill?

Ms. HUGHES. I believe, Representative Pallone, that you have hit upon the single greatest challenge from the consumer perspective. And this particularly affects unbanked and underbanked individuals. So the persons who are using credit cards and debit cards have access to two Federal statutes that have been in place, in one case, for more than 40 years and, in the other case, for 37-plus years: the Fair Credit Billing Act and the Electronic Fund Transfer Act. You are correct that their standards are slightly different. You have to report faster on an EFT transaction than on a credit card transaction, and your liability can be different, although Visa and MasterCard on the credit card side have a no-liability policy. And PayPal, as I remember since I am a PayPal user, does have a no-liability policy, and there are other opportunities.

The consumer, however, who is billing to a mobile phone statement, as opposed to using a financial institution for the clearing and settlement of the payment they are making, does not have the same level of protections because those are both either because there is a credit card present or a bank account present. And so the credit and debit cards are access devices to those two different kinds of accounts that many people who are unbanked—certainly they won't have debit cards—although they may have prepaid or payroll cards. And the prepaid and payroll cards are increasingly being brought under the Electronic Funds Transfer Act.

So the key gap at the moment is the person who is billing something to their mobile phone account without some other financial services provider doing the clearing and settlement for the payments. And that is the gap that exists in Federal legislation right now, and that is a gap that also exists in the States.

Mr. PALLONE. So you said that with prepaid cards—and what about gift cards—there is some protection?

Ms. HUGHES. That is correct. Not all of the electronic fund transfer protections currently extend to gift cards. Some of the issues about dispute resolution do not extend all the way through the gift card family at this stage, but payroll cards have better protections than regular gift cards do in the same environment because of efforts to bring them under the Electronic Fund Transfer Act.

Mr. PALLONE. What do you suggest that we do legislatively, agency action, whatever, to have the strongest protections for all these different things, particularly the ones that have the lesser protection, based on what you said?

Ms. HUGHES. Well, one issue which this committee doesn't have is jurisdiction, so the Federal Trade Commission doesn't have jurisdiction over carriers for that purpose, for example, and I don't be-

lieve the CFPB does either. The States, because of the strength of the Federal Communications Act, I don't think the States have authority to do all of this work. If you wanted to do that, I think it would be up to Congress to instruct the Federal Communications Commission, giving them some additional authority to play in that realm, or to extend the reach, if you felt it was important, to extend the reach to persons who do not use financial institutions and access devices to accounts, either credit cards or debit cards, to have comparable protections. I haven't thought about exactly what those would look like, but I think it is an extremely interesting topic.

Mr. PALLONE. I have just a little time.

With so many vendors and third parties involved in some of the mobile payment transactions, I was concerned that consumers could be given the runaround, in other words, each vendor pointing the finger at the other? Do you want to just comment on that? We only have just a little bit of time.

Ms. HUGHES. I think that the consumers may go to vendors for that purpose, but I think consumers largely go to their financial service providers, whether, it is Samsung and PayPal or their bank, to get resolution of disputes. The one gap you have identified, sir, is the one where they are not going to have that person to help them——

Mr. PALLONE. OK.

Ms. HUGHES [continuing]. Not in the same fashion.

Mr. PALLONE. All right. Thank you.

Thank you, Mr. Chairman.

Mr. BURGESS. The gentleman yields back.

The Chair thanks the gentleman. The Chair recognizes the other gentleman from New Jersey, the vice chair of the subcommittee, Mr. Lance, 5 minutes for questions.

Mr. LANCE. Thank you, Chairman Burgess.

Ms. Deckinger, it is apparent that one of the biggest hurdles to getting consumers to adopt a certain payment method is scale. What steps need to be taken in order for a payment method to be accepted with enough ubiquity that consumers find it to be beneficial? And, from your perspective, are there any legal impediments in order to make sure that this is the case that we can move forward?

Ms. DECKINGER. Thank you so much for your question. We believe, fundamentally, that you have to have what I mentioned earlier, which is muscle memory for consumers. They are very comfortable with our current forms of payment. They are very comfortable going to a store and striping a credit card. It is not difficult for them. So getting them to change that behavior we believe requires having a presence at places where they shop every day and multiple times.

We believe that our network includes that kind of scale and has that great reach. Consumers are gassing up at fuel stations several times a week if not at least once a week. They are at coffee shops. They are at their big retailers doing their grocery shopping. We feel like having that scale is really going to drive that adoption and regular usage that will create that muscle memory for consumers to get used to using a new form of payment.

I don't currently feel that there are any legal restrictions that are keeping us from getting that kind of scale, but I would welcome other input on that.

Mr. LANCE. Yes. Anyone else on the panel?

Professor Hughes?

Ms. HUGHES. I would agree with Ms. Deckinger that there are no legal imperatives or hurdles to the greater adoption. As I mentioned earlier in response to a question from the chairman, I believe it is one which may involve consumer education more than anything else. And I think that the—it may also be generational. And so I think it is a— millennials are much more likely to use mobile payments than older people. My late mother, who was very clever, never used an ATM, not because she didn't feel like it, just because she wasn't a particularly mechanical person, and I think she was comfortable with the option she had. And the comfort level with the options that are currently available, even though they are expanding, is a difference between us and other parts of the world where the banking system is not as robust, where the penetrations of the Samsung and PayPal style opportunities are not as great, and where, in the case of some, you have to have a smartphone, and a new enough smartphone to use it. You are going to see in older generations and in less affluent generations lots of smartphones, but not everybody has one. And so the mechanical barrier may be, depending upon the nature of the service being offered, the mechanical barrier of what kind of device you have available for this purpose, which is something that just takes a maturation of a marketplace.

Mr. LANCE. Thank you. Mr. Muller, you said how many transactions from PayPal a year? A billion, did you say?

Mr. MULLER. A billion in 2014. That is right.

Mr. LANCE. And there will be more, you believe, this year, because in your last quarter, it was 350 million or something like that.

Mr. MULLER. That is correct.

Mr. LANCE. What percentage are in the United States? And what percentage are in Europe? And what percentage are in Asia?

Mr. MULLER. So our largest markets overall in the world, you know, are by and large the English-speaking countries: U.S., U.K., Canada, Australia, also Germany. And in all of them, we see pretty comparable rates of mobile payment as a proportion of total payment, so getting toward a third of all of our payments are on a mobile device, again, usually either a phone or a tablet that is used where 5 years ago, it would have used a laptop or a desktop.

Mr. LANCE. Thank you.

Mr. Ahn, explain Samsung's latest device. In your testimony, what did you say that Samsung is doing next? Samsung Card? Samsung——

Mr. AHN. So the question is with respect to our products——

Mr. LANCE. Yes.

Mr. AHN. In the ecosystem?

What we are doing today is we have reflexive devices, which we call Galaxy and Note. We are looking at future devices and a broader ecosystem where we can put Samsung Pay onto them,

whether they are additional mobile devices or even wearables. We are looking at a broad ecosystem.

Mr. LANCE. A wearable would be a——

Mr. AHN. A watch.

Mr. LANCE [continuing]. A watch? And you can then purchase items or pay for items from that device?

Mr. AHN. That is part of our thinking.

Mr. LANCE. Has that occurred yet, or is that still in development?

Mr. AHN. We are evaluating and developing now as we speak.

Mr. LANCE. Thank you. And thank you for making New Jersey your headquarters in this part of the world. We deeply appreciate that. And I have been at your world headquarters in Seoul and have been deeply impressed with them.

Thank you, Mr. Chairman.

Mr. BURGESS. The gentleman yields back. The Chair thanks the gentleman.

The Chair recognizes the gentlelady from New York, Ms. Clarke, 5 minutes for questions.

Ms. CLARKE. Thank you, Mr. Chairman. And I thank our ranking member.

Transparency. Unlike simple cash transactions, using a mobile payment system can bring in unseen third parties. So Professor Hughes, it seems like there are often many entities involved in mobile payment transactions than consumers may realize. How can we assure consumers know who is involved in their mobile payment transaction apart from themselves and the service that they are directly interacting with?

Ms. HUGHES. Representative Clarke, that is a very interesting question, and I believe it is one to which we do not have a very clear answer. So I think that there are systems that operate, particularly apps, not services of the kinds being offered by PayPal and Samsung. And where the app is involved, it is much more likely that there are unknown third parties involved in processing for the merchant, particularly, because merchants use a lot of third-party payment processors. And third-party payment processors are among the least regulated entities in the payment space today. They are not very well regulated by the States. Some of them are regulated as money transmitters; some of them are not. And they are not particularly well addressed by congressional legislation to this point.

Asking the merchant, for example, or the app provider to make that kind of disclosure could possibly be more burdensome than it would be worth. So I think it is more important to ask—and each of these groups and others do—for people to engage in robust supervision of the choice of providers that they use along a tract that may be involved and to supervise them appropriately for risk-management purposes.

The members of this panel might not be excited, but you might care to read a study that was issued in August of 2015 by The Clearing House payments company on, which I would be happy to provide to your staff if someone tells me to which person it should be sent. That study talks about this issue in particular in greater depth than I have time to do this morning or you do. And so I

would suggest that it might be something that you would read on that particular narrow subject, which is quite an important one.

Ms. CLARKE. So let me——

Ms. HUGHES. I urge you not to make it too complicated because people choose providers based on their histories with them, and it would be very difficult to make new disclosures constantly if you had to abandon a provider because they didn't behave appropriately and choose a new one——

Ms. CLARKE. I think we are concerned more about breaches. You know, you are then dealing with many more entities that are holding the data, right?

But let me move to ask about lack of transparency and consumer consent, the notion of consumer consent.

How can consumers consent to business relationships with entities that they are unaware of?

Ms. HUGHES. Well, Representative Clarke, that is a very complicated question. And I think that as there are already lots of payment processors operating in the United States where we are not seeing a lot of transparent consent, I think that it may be the necessary level of consent, maybe the consumer who chooses the payment method and the consumer who chooses the merchant at this point. And I firmly believe that the mechanics of this are such that we should put the primary focus on the merchant to choose wisely and on the payment provider to choose wisely and to ask them to perform the functions that are currently present in Federal and State law to supervise them.

Ms. CLARKE. Do you believe that greater transparency could encourage more consumer use of mobile payments? Because, certainly, consumers who are unwilling to use mobile payment services may feel unsure about who will have access to their data afterward.

Ms. HUGHES. That, too, Representative Clarke, is an excellent question. And I think the more that consumers understand how mobile payments work, as a general, as opposed to a specific proposition, but perhaps both, the more they are likely to be willing to use them because just like ATMs 40 years ago, there was a period of adoption, and it made a difference when consumers——

Ms. CLARKE. But ATMs don't have a third party. You know you can just walk into that——

Ms. HUGHES. Some do, actually.

Ms. CLARKE. Absolutely, right. Absolutely. Clearly.

Ms. HUGHES. Kiosks in stores and other places have a landscape and an ecosystem that is very much like mobile payments today. So the answer is, but there, you are talking about your bank, and you are talking about the place where you use the machine, assuming you remember where it is, and it is usually on your receipt. So I am not sure that that is so much different than what consumers are already dealing with with a fair amount of comfort. I just think they need more education.

Ms. CLARKE. I yield back. Thank you.

Mr. BURGESS. The gentlelady yields back. The Chair thanks the gentlelady.

The Chair recognizes the gentleman from Mississippi, Mr. Harper, for 5 minutes, please.

Mr. HARPER. Thank you, Mr. Chairman. And thanks to each of you for being here.

I guess I would have to say that I never envisioned the title of mobile payments would be exciting, you know. So it is an incredible topic, and it is affecting our lives in so many ways as we look at this. And so I am all in. This is a great topic.

Mr. Muller, if I could start with you. In your testimony, you mentioned that PayPal has been involved in mobile payments innovation since the PalmPilot devices. What have been some turning points that you have seen in the development of mobile payments from PayPal's perspective, and what are the next big applications that we should be on the lookout for?

Mr. MULLER. So, you know, like most companies, there have been some successes but also some learning opportunities. One was, as I mentioned, the switch away from the PalmPilot as the focus towards email and Internet connection. A second generation really starting, I think, in 2006, we launched a mobile payment feature available to users to make payments mostly intended for person to person, but a few also businesses had signed up using text message and just sending a text message with the amount and a certain code in it. And that, frankly, was not very successful I think largely for some of the reasons that have come up about security and many consumers just feeling a little bit too uncertain that just by pushing a text message, the money would go to the right place and be credited correctly.

So that——

Mr. HARPER. Does that mean it was too simple to give confidence?

Mr. MULLER. Well, I think perhaps to some degree, I don't know if too simple or simply too unclear, too little information associated with the actual transaction itself. And this was at a time just before the iPhone. So we are still talking about flip phones and other types of phones with very small screens.

So the whole texture of the experience, to some degree, was not as comforting as is available today with smartphones and larger screens.

So I think we have learned that lesson, and a big part of what we have done that got to us to the 1 billion transaction number that I mentioned is not just building mobile apps and experience on the consumer side, but also helping our merchants, who are, by and large, mostly small- and medium-size businesses optimize their Web site and their checkout pages for mobile devices so that the experience is as good as it can be on the smaller screen.

Mr. HARPER. So what is the next big thing to look for? Where are we headed?

Mr. MULLER. Well, so one thing that is already live for us—and it is an experience, again, that many other payment companies are also in their way matching or trying to—is what we call the one-touch experience, taking advantage of the information that the consumer has chosen to share with us, recognizing them the next time they go shopping even at a different merchant than they have shopped at before. We can recognize them so they don't have to type in information on a small screen. We can recognize them if they have chosen to opt into this feature and, again, improving

both the shopping experience and the merchant checkout. And then the other set that is coming out, say, is at the point of sale, where to date, you know, certainly PayPal is less prominent, but finding that right match of convenience and merchant acceptance and speed and security, something all of us are working on, and that is coming. Just who unlocks the right combination is yet to be seen.

Mr. HARPER. You know, our time is almost up. But one phrase that was of interest was in your testimony; you note that 17 of the 100 most unbanked places are in Mississippi. How do you envision mobile payments increasing consumer options in those communities?

Mr. MULLER. So that is another challenge for the industry as a whole that we are eager to take on and do more. Today, I would say, really, that the primary vehicle linking the unbanked to mobile transactions is through prepaid cards or prepaid accounts of different kinds that different providers are offering. You know, and there are, of course, starting with the baseline that many of the financially underserved today do have smartphones.

Mr. HARPER. Mr. Muller, I apologize. My time is well over.

Mr. Chairman, I yield back.

Thank you, Mr. Muller.

Mr. BURGESS. The gentleman yields back. The Chair thanks the gentleman.

The Chair recognizes the gentleman from California, Mr. Cárdenas, 5 minutes for questions, please.

Mr. CÁRDENAS. Thank you very much, Mr. Chairman. And thank you to all the witnesses that are here enlightening us of what has been, what is, and even what may be coming in the future.

But I think the main concern of this committee is the safety and security of Americans and people in our country, whether they are visiting or what have you, making sure that they feel comfortable and confident that we have a system that actually works and hopefully works for as many people as possible.

Speaking of as many people as possible, there are still many communities here in the United States of America that are underbanked and underserved by financial institutions and instruments, et cetera, so they tend to not experience or see the safest and best technologies and, unfortunately, sometimes actually are subject to more problems because they don't have the best systems available to them.

That being the case, when it comes to these kinds of communities, how can mobile payment providers better reach minority communities and underserved or poor communities and ensure that these consumers also enjoy the safe and community commerce that everybody else expects or can experience?

The main thing there is, certainly, if there is a community with a lot of wealth and a lot of activity and probably a bigger contributor to the billion transaction mark, you have other communities that want to participate, yet, at the same time, how do we make sure that we have an even system that is available to them, really?

Professor?

Ms. HUGHES. Well, I think this is a truly important challenge. And I think that mobile payments are an enormous opportunity to help unbanked and underbanked individuals. Unbanked individ-

uals don't have bank accounts. Underbanked individuals may just not have a bank very close by. And if we think about the ability of someone to make a payment remotely or to take a payment from an employer or to pay their rent using their mobile device and not having to take time off from work to do that or to take time to go to the bank to deposit checks and the like, I think that the underbanked communities that have bank accounts or other credit union accounts, et cetera, but may not have time to get there during reasonable work hours are among the communities that will benefit the most from mobile payments.

I think the opportunities in those markets are huge. I think they will help the citizens of Mississippi and California and the other jurisdictions that are here. They will help inner city people as well, people who no longer have a corner branch of a bank to help them. And because, as Mr. Muller suggested, there are opportunities to use prepaid cards, including payroll cards, and to spend money out of them using devices of this kind, the opportunities for unbanked and underbanked persons and minority individuals residing in rural or very urban communities expand.

The last thing I would say, sir, is that the least secure thing on the face of the planet in the United States, as least, is cash. So if you have a way to link to some form of an account and to use it as if you were using your bank account through a mobile payment, you may level the field for lots of people to participate in commerce, both the recipients of payments and as people who can make payments on time and, therefore, avoid late fees and other charges that are associated, and that these opportunities are enormous for helping a lot more Americans have a lot better access to payment options than they have had in the past.

Mr. CÁRDENAS. Well, my last question, because our time is limited, is it is interesting that "60 Minutes" talked about this payment system in Kenya that you touched on, Mr. Muller, that has to do with the texting, and it doesn't have to be a smartphone, et cetera. The thing that concerns me about that isn't that it is kind of cool; it is that I would imagine that the safety of those individuals in those transactions are a lot more vulnerable than, perhaps, what Americans understand that we are not as vulnerable with the systems and the advances we have.

I would like to know, as quickly as possible, due to constraints of time, the fact that in this country, we do have regulations and we do have benchmarks and push industry to make sure that they have safeguards for our consumers and our participants, is that something that is helpful to the industry? Or is that something that you can do without?

Mr. MULLER. So I would say, certainly, it is helpful, in general, of course, the right kind of regulation. But, in general, regulation is certainly one component that leads to consumer adoption. And, as you said, if people viewed these kinds of transactions as really, the same as cash with no purchase protection or no protection against unauthorized transactions, they would be much less inclined to use it.

So regulation is one component of addressing that issue. Industry efforts, like Visa and MasterCard and PayPal, zero liability, all come together to lead to the broader mobile adoption for all of us.

Mr. CÁRDENAS. Thank you.

I yield back my time.

Mr. BURGESS. Thank you. The gentleman yields back. The Chair thanks the gentleman.

The Chair recognizes the gentleman from Kentucky, Mr. Guthrie, 5 minutes for questions, please.

Mr. GUTHRIE. Thank you very much. It is neat having this hearing today. I was flying back yesterday reading a biography of Andrew Jackson, and it is amazing moving an army, speculating land, all the others things that he did. One of his biggest concerns was always how did he move currency, cash, how did he pay people. Was it going to be barter, bank drafts? It was just a big issue then. And so how currency moves really played into how he was able to move his armies and so forth back and forth. So we are still talking about moving currency, and how we move it in the best and most efficient and safe way.

And I was watching, I guess, a football game or so this weekend. And Samsung had their advertisements. They must have bought a lot of time because I remember seeing the app that we are talking about here today. And I grew up in a rural grocery store, so I always view things through rural, kind of, groceries. So it appeared that anywhere that you can do a credit card, your phone would work. So if you can pay at a pump, then you can actually scan or whatever the technology is, if I am using the right term, then your phone works in all applications like that? So if any merchant takes a credit card, then you have the ability to use your application? Is that——

Mr. AHN. So, Congressman, thank you for the question. When we say virtually anywhere, what we are talking about is very, very high percentage of locations and terminals that accept any credit card or debit card. However, we say "virtually" because we are not fully 100 percent there. There are instances such as DIP readers, gas stations, ATMs, and a small percentage of merchants where the technology software needs to be upgraded for us to get to everywhere. And so we are not quite there yet, but we are substantially ahead of our competition.

Mr. GUTHRIE. Well, thank you.

My first question was your level of mixes of security and how it protects consumers. You answered that with Mrs. Blackburn, I think.

So does it prevent the consumer from doing it to themselves, I guess we would say? Are there things the consumer needs to do? Once they use your phone, your phone is—can the consumer—like if, the old days, when you swiped a debit card and you didn't throw the receipt away and somebody took it out of your garbage or you didn't tear it up, is there something like or equivalent to that the consumer can do, or have you protected them from all aspects?

Mr. AHN. So the consumer is essentially protected behind a level of password protection and fingerprint indication that is required to open up the app. And, therefore, everything that they are doing is really sitting behind that level of protection. We don't publish that information. It is not easily accessible. And the consumer really has full control over that. So, to that extent, it is secure.

In terms of usability, I think all mobile payments have usability issues because people are—for the most part, their muscle memory today is credit card and debit swipes, and so it is going to take the ecosystem to work together to help educate consumers about the advantages of having more secured payments and a new way of tapping, a new way of paying. This is happening in different parts of the world. Western Europe, for example, is actually more tap-centric payment countries. In the U.S., we are further behind.

However, you know, as a technology company, we are very optimistic about technology advances. Five years ago, the cell phone, smartphone penetration was very different than it is today. New applications of services are quickly adopted if they are helpful and make an impact. So we are hopeful that there is enough security, utility, and a better experience to compel consumers to move toward a more technology-centric way of paying.

Mr. GUTHRIE. Thank you.

And, Mr. Muller, I understand that PayPal utilizes the cloud for storage of consumers' payment information. And why did you choose to utilize the cloud instead of storing payment information on the phone or the app? Is it more secure, I guess, is the question I am getting at?

Mr. MULLER. Well, for us, it was partly out of necessity in that we don't have the same access to mobile phone hardware and operating system that some of the other companies that are operating point-of-sale payments through a mobile device do. But, also, we do think there are some advantage of storing the information in the cloud and not—certainly not storing any of the information on the device. I mean, that is clear, and that is undesirable. But, also, we don't have the same access to the device as the handset manufacturer might.

Mr. GUTHRIE. So being in the cloud, you are obviously—PayPal is not a device. You are not device-specific. That is your——

Mr. MULLER. Yes.

Mr. GUTHRIE. So what innovations have you seen over the last year or two that would make online payment data more dynamic and less useful for criminals?

Mr. MULLER. Well, so, certainly, tokenization continues to develop. It just started, so it is certainly not static by any means. But the first, really, live implementation of tokenization in a practical way that we have seen is a big step forward, and the controls that can be built in for one-time use of the token, merchant-specific use of the token, all those are certainly, a step forward compared to where we have been with the primary account number being stored and transmitted in many ways. So that is probably a major recent development.

There are new ones coming out all the time that we read about. So it is an exciting field with, certainly, dynamic codes. Sort of the three-digit or four-digit code in the back of your card that you are used to entering, now companies are coming up with a capability to generate that dynamically and change it for every transaction. So certainly new developments are coming out, and there will be more to come.

Mr. GUTHRIE. Well, thank you. And I only have 15 seconds. I am not going to ask another question.

I yield back, Mr. Chairman.

Mr. BURGESS. Thank you.

Mr. Kinzinger.

Mr. KINZINGER. Thank you, Mr. Chairman.

And thank you, all, for being here. I appreciate it. The innovation of mobile payments is at the forefront of many consumers' minds, especially those that were considering purchasing a new smartphone and all consumers interested in the technology to ensure their transactions are safe and secure.

Like with many new technologies, it is subject to some suspicion before adoption, and many consumers want to know if their personal information, including financial and personal health information, will remain protected and private.

Certainly, no system is foolproof. In the technology world, we frequently read about cyber attacks and successful hacks of various systems. Consumers have a right to be concerned about new technology, but I am hopeful that today's conversation will showcase some of the great strides in technology that we have made and what its future could look like.

Mr. Muller, the number of smartphones in the U.S. continues to grow, and obviously, mobile payments are increasing in popularity. Over the course of PayPal's involvement with mobile payments, what have been the largest keys to consumer adoption, and what have been your biggest challenges?

Mr. MULLER. So, certainly, one of the keys is the one you mentioned, which we certainly can't take credit for, but is the proliferation of the smartphone and the affordable smartphone through the work of the handset manufacturers and the mobile carriers, and that is probably—that is the baseline for all adoption that we have been talking about.

And then, really, there is just the passage of time, as we have seen with other payment devices. Professor Hughes mentioned the ATM card, the credit card, the debit card as a purchase device.

Consumers get comfortable through word of mouth, through—there are always early adopters, and that is one of the things we are lucky to have in the U.S. is people who are eager to try new things, and if it works for them, to spread the word.

And then, ultimately, another important factor has been merchant adoption and getting the merchants to realize this is something that is good for them as well. It creates a good experience for their buyers and ultimately more transactions for them. And so just that extra nudge from some of the merchants to encourage their consumers to try their app on the mobile phone, that can be the deciding factor for many consumers.

Mr. KINZINGER. And you also, you know, you obviously, described, that when you started up, you called it, basically, an early form of tokenization. Very like 50,000-foot level. Can you just briefly describe how your security methods have evolved over the years from 16 years ago to today? I know we can talk for hours about it, but——

Mr. MULLER. Well, as I said, the basic component and what we were referring to as that early form of tokenization is just not creating a process where the merchant receives the card number in the first place. So, with PayPal, they receive news of the payment

in the form of either an email; or, for some more advanced merchants, they might receive an automated notice to their systems; or they can just go look at their account to see that the payment is there. But, in any case, they are not receiving the consumer's card or bank account information to start with. So that is a similar concept to what tokenization is now achieving more broadly.

That, of course, makes it incumbent upon us—we are receiving the account information—to protect that account information. We had the good fortune, as one of our founders was and still is a computer security expert and designed the system in a solid way. And, of course, as I said earlier, continuing to make investments on that foundation for both encryption of the data and limited access even by employees to the data.

Mr. KINZINGER. Well, Mr. Ahn—I hope I said that correct—some of the security concerns that I have heard raised with the NFC-based mobile payments has been eavesdropping, data manipulation, interception attacks, relay attacks, and device theft. Can you discuss if these are real concerns or misconceptions and perhaps how the Samsung Pay approach addresses some of these?

Mr. AHN. Some of the concerns you mention are real; some are misconceptions. The real concerns are related to device theft and loss that relate to relay or replay attacks. There are a number and a host of ways that fraudsters can steal information, and our job is to be ever-vigilant and put the best and most advanced security features in cooperation with our partners, with banks, the Visas, MasterCards of the world, the networks, and make sure that we have as much fortification as possible.

With respect to Samsung Pay, we have looked at every possible angle of security, and it starts, again, as I mentioned before, at the baseline level, moves all the way up. We are very, very concerned about security.

As a matter of background, Samsung is one of the most respected brands around the world. We have a very strong relationship with a large base of consumers. That relationship and trust and brand is sacrosanct to us. We will not jeopardize it. And so when we think about what we put into market, we will index heavily toward security. And, yet, as a viable consumer solution, we have to have it usable and simple. And so that is our challenge and our burden to bear.

And so we take that very seriously, and we would be happy to share addition information in more detail.

Mr. KINZINGER. Thank you, Mr. Chairman. Thank you for your leniency. I yield back.

Mr. BURGESS. Thank you very much.

Congresswoman Brooks.

Mrs. BROOKS. Thank you, Mr. Chairman.

This past August, I had the opportunity to visit Tanzania, Africa, where I saw the majority of the population utilizing mobile payments and paying for everything from cabs to a dinner tab to hotel stays, and so the mobile payment technology I think is incredibly advanced in Africa. And we know that in a large part of sub-Saharan Africa, traditional banking has been hampered by a lot of infrastructure problems and transportation. And we now know that so many people worldwide, approximately 2.5 billion people, don't

have formal accounts at financial institutions, as Professor Hughes touched on. It is allowing these communities to provide for the unbanked and the underbanked individuals and businesses to conduct business.

And so I am curious, though, how it is that Africa, in many ways, has leapfrogged over the United States in using this technology? And it was being used in the smallest of shops and to the large hotels. And so I am curious, particularly, for anyone with any—companies with the international background, how and why did that happen? Mr. Ahn?

And what should we be thinking about in seeing that, you know, other countries—and I am talking about visiting with people in huts that didn't even have significant access to electricity at times. And so a lot of them were charging their phones with solar-powered devices and so forth. But how is it that Africa has, I think, advanced so much faster than we have?

Mr. AHN. So, Congresswoman, one thing I would add is the examples in Africa highlight that necessity is the mother of invention. In Africa, the financial institutions and the infrastructure for typical banking is at such a state of underdevelopment that those in need of payment remittance, access to funds, needed to find some other way to move money around, pay each other, and to conduct commerce. And so these payment solutions on pace in Kenya and other leading applications leapfrogged the need for established banking institutions in such a way to create viable payment commerce.

And I think the relevant piece of what we have learned in developing countries for us is the question that the Congresswoman asked earlier with respect to how we serve our underbanked populations and provide access to as many people as possible for these payment solutions.

For us, we argue that mobile changes everything. Mobile does not tie you down to location or place.

As Ms. Hughes was saying, you can, at your own time, at your own choosing, and location, conduct transactions and services that are important to you and have access on a more equal playing field than if you were tied to time and place. And so when mobile is coming into the picture, we believe that our job now is to then open up access to the services and solutions that we can make an impact for consumers. The way we think about it is we have a large device footprint. We want, as I mentioned in my testimony, we have plans to continue to evaluate broader ways to provide Samsung Pay on more devices. One very easy way to do so is when previous generation phones are in market, they come down in price point, making it more accessible for different consumers. In addition, we know from our own data that Samsung as an OEM has one of the highest percentages, if not the leading percentage, of share of market in underserved populations as well as lower income populations. And then, on top of all of this, the way we have constructed our solution is to open our doors for all payment types. What that means is that we can support credit cards, debit cards, prepaid cards. We will roll out in the near future gift cards. We have every opportunity for any payment instrument in any tendered type to be usable in our device. So that is how we think about this.

Mrs. BROOKS. Thank you.

Professor Hughes, I am curious what you believe the impact is going to be for this type of payment method for the—is there going to be any burden of entry for entrepreneurs who are just starting businesses, or do you think this will be beneficial to them?

Ms. HUGHES. Congresswoman Brooks, I think this is a boon to small business. I think, as I mentioned earlier, it is a boon to farmers markets and artisans and music festivals like we have in Bloomington, Indiana, and arts organizations and charitable causes around the country. I think particularly for smaller businesses, this is an enormous advantage because it will allow them to take payments that they may not have been able to take before in a speedy and secure environment.

And I think that we should be optimistic about the future of mobile payments and their ability to serve underbanked, unbanked, and small business.

Mrs. BROOKS. Thank you. Thanks for your testimony.

I yield back.

Mr. LANCE [presiding]. Thank you.

Mr. Olson.

Mr. OLSON. I thank the Chair.

And welcome to our witnesses.

I have a challenge for you, Mr. Ahn, Ms. Deckinger, and Mr. Muller. In preparing my questions for this morning, this testimony, I relied on advice from people here in DC, lots of folks back home, and two of my own personal experts, my two teenagers, my 18-year-old daughter and my 15-year-old son. They are all about mobile. That is all they know. And they are current and future consumers, big consumers.

So, Mr. Ahn, can you explain how your mobile technology works that I can show my daughter and my son, explain to them and their friends, "Hey, Samsung has got this great vision"? What can I say to my kids? How could you explain it in English?

Mr. AHN. So, apparently, the previous testimony was——

Mr. OLSON. No, it was good. It was good for DC. I want to make sure my kids understand this because they are the future.

Mr. AHN. So the young population is an important demographic to follow. What they do and what their habits are, are leading indicators of what new consumer trends will be. For them, what is important is the ability, I think, to focus their life around services and goods that revolve around mobile devices. Our view is that we want a future where consumers have the ability to pay in a store offline, inside an application, an app, let's say an Uber, or a mobile-Web context. Anywhere you are, in any space that you are, we want you to be able to pay with the secured credentials that you have loaded. So we have that opportunity as we build out our product roadmap.

What the Samsung phone allows you to do is to take a credit card or debit card or any other payment instrument, put it into the phone, and make a secure payment at the terminal. Over time, we expect to create more intelligent services that create more consumer impact, things that we can't discuss today. But over time, we expect that the ability to pay in a secure method with a phone

allows you—allows us to open the door for new innovations that will have a direct impact for them.

Mr. OLSON. Is there any PII left after—PII, personal identifying information—after a transaction with your mobile system?

Mr. AHN. There is no PII except for you do know that the phone belongs to a certain user; traditional information is already there. But no additional information is left.

Mr. OLSON. Mr. Muller, same question. Explain to my kids, how does PayPal's system work, and is there any PII involved after the transaction?

Mr. MULLER. So, PayPal's system, you know, works somewhat differently, or it is not tied as closely to the physical device. It does involve working through an account that has to be set up to start with either by the individual themselves if they are over 18, since that is one of our rules——

Mr. OLSON. One is there, one is not.

Mr. MULLER [continuing]. Or by their parents. We do offer a student account capability where parents can control an account on behalf of the student. But there is that initial step of setting up an account. Once the account is set up, we then have a broad network of merchants that the user can access through their mobile device, through their laptop, or other kinds of device. So it becomes very easy to make that payment once that initial step of setting up the account.

Mr. OLSON. Any PII left over after a transaction with PayPal system?

Mr. MULLER. So, you know, the PII is something that is kept only by us, so we do have it, and we do have the information, and then the merchant has what they need. If they are shipping physical goods, inevitably that means they need a physical address to ship it to.

But, really, that is the extent of the information.

Mr. OLSON. And, Ms. Deckinger, you are the new kid on the block. How does currency envision its testing phase, and can you explain how your mobile technology works for my daughter and son?

Ms. DECKINGER. Yes. We have some pretty cool technology——

Mr. OLSON. I like it already, the word "cool."

Ms. DECKINGER [continuing]. That would help ease the path. One of the great things we have, for example, is Pay at Table. So that frustrating experience when you are at the end of the transaction in a restaurant, sitting in a restaurant, and you want to pay your bill and you are waiting for the server to come over and bring your bill, we allow you to scan the QR code that is on the receipt, pay and leave without having to do that. We allow to you stay in your car when it is 100-plus degrees in Texas and pay from the comfort of your car.

Mr. OLSON. Thank you.

Ms. DECKINGER. And we allow to you pay at the drive-through without handing a card out the window to the person on the other end. Pretty cool thing, the phone actually that when you pay at drive-through is pinged through the Bluetooth low-energy beacon, so that is a fairly cool technology that your teenagers will find fascinating. And PII was the other question.

Mr. OLSON. That is a—yes, ma'am. How are you guys planning on protecting that if you have any after-transaction left over? So like Mr. Muller——

Ms. DECKINGER. Similar to Mr. Muller, there is some PII involved. However, we do not pass any financial information through the transaction. So we use tokenization, everything from a financial perspective is tokenized and encrypted. So that means that there is never any financial information stored on your phone, nor information that is of worth to anybody to store on your phone. So should your phone be stolen or hacked or taken by someone nefarious, nothing can be done with it.

Mr. OLSON. Thank you. My time is up. My kids would be very happy. Thank you, all.

Mr. LANCE. Thank you, Mr. Olson.

Mr. Welch.

Mr. WELCH. I got here a little late. I missed—would you like me to comment?

Mr. LANCE. Very good.

Is there anyone else who would like to ask questions?

Thank you.

I thank each of the members of the panel for participating. I think this has been a very interesting and informative hearing. Before we conclude, I include the following documents to be submitted for the record by unanimous consent: a statement from the Electronic Transactions Association; a statement from the National Association of Convenience Stores and the Society of Independent Gasoline Marketers of America; and a statement from the National Retail Federation.

[The information appears at the conclusion of the hearing.]

Mr. LANCE. Does the ranking member have anything that should be included in the record?

Mr. SCHAKOWSKY. I don't, but I approve all those inclusions.

Mr. LANCE. Thank you. Pursuant to committee rules, I remind Members that they have 10 business days to submit additional questions for the record. And I ask that witnesses submit their responses within 10 business days upon receipt of the questions.

Without objection, the subcommittee is adjourned.

Mr. SCHAKOWSKY. Thank you.

[Whereupon, at 12:15 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]



1101 16th Street NW
Suite 402
Washington, DC 20036

www.electran.org
800.695.5509
202.828.2635
202.828.2639

Statement for the Record

Electronic Transactions Association (ETA)

BEFORE THE

United States House of Representatives

Committee on Energy and Commerce

Subcommittee on Commerce, Manufacturing, and Trade

"The Disruptor Series: Mobile Payments"

December 1, 2015

ELECTRONIC TRANSACTIONS ASSOCIATION
1101 16th Street NW
Suite 402
Washington, DC 20036
www.electran.org
800.695.5509
202.828.2635
202.828.2639

The Electronic Transaction Association (ETA) is pleased to present this statement for the record before the Committee on Energy and Commerce's Subcommittee on Commerce, Manufacturing, and Trade on its hearing on Mobile Payments. ETA is a global trade association whose mission is to advance the payments technology industry. ETA represents more than 500 of the world's most innovative payments and technology companies, from Fortune 500 financial institutions and the largest technology companies to small, local sales organizations. ETA's members are dedicated to providing merchants and consumers in our country the safest, most reliable, and most secure payments system to facilitate commerce and power our economy. The first three witnesses, PayPal, Samsung, and MCX, are ETA members.

With this goal in mind, ETA's Mobile Payments Committee works to identify and address critical issues facing the future of mobile payments including the development of best practices and guidelines to ensure that consumers and merchants have access to innovative and effective mobile payment solutions. The Committee also attempts to educate consumers and merchants on the potential of mobile services to provide a more efficient, reliable, and secure means to expand commerce.

DISRUPTION BY INNOVATION – THE BENEFITS OF MOBILE PAYMENTS FOR CONSUMERS AND BUSINESSES

Our statement focuses on some of the many benefits that mobile payments provide for consumers and businesses. In the terms of today's hearing, mobile payment technology is "disruptive" in the sense that it plays an important role in expanding the accessibility of convenient, cost effective, safe, and diverse payment options. Mobile payments and financial services give consumers unprecedented ability to pay for transactions and manage their spending and finances. Using a smart phone, consumers can quickly and securely pay for a holiday gift for a friend or a bill they forgot was due, check their bank balance while on the go, and even receive discounts based on their location.

In just two decades online commerce has grown from approximately $5 billion to more than $263 billion today. Similarly, mobile payments have been growing and are poised for wide-spread adoption with the recent introduction of a number of new payment platforms. Approximately 87 percent of U.S. adults have a mobile phone and 71 percent of these phones are smartphones.[1] According to a recent Federal Reserve report, 28 percent of smart phone users reported having made a mobile payment in the past month.[2] This revolution in technology and business has benefited, and will continue to benefit, consumers and business by providing efficient, convenient, and safe payment options.

1. Mobile Payments Provide Consumers with Access to Convenient, Diverse, and Cost-Efficient Payment Options

Mobile payments provide secure, cost-effective, and flexible payment options for consumers and businesses. To the extent that these products are disruptive it's because they increase

[1] Federal Reserve Board of Governors (2015). Consumers and Mobile Financial Services.
[2] Id.

ETA
ELECTRONIC TRANSACTIONS ASSOCIATION
1101 16th Street NW
Suite 402
Washington, DC 20036
www.electran.org
800.695.5509
202.828.2635
202.828.2639

competition by providing consumers with additional payment options. Such competition not only benefits consumers by providing another payment method, but also pushes the payments industry as a whole to provide the best possible products and services for consumers.

Mobile payment systems are secure, easy to set up, and can be accepted virtually anywhere you can swipe or tap a credit or debit card. PayPal, for example, offers consumers a "digital wallet" that connects into and leverages traditional payment networks, enabling PayPal's users to send and receive payments in a safe, secure, and efficient manner, including through their smart phones. The development of these and other similar mobile technologies has grown rapidly because consumers value the benefits provided, including accessibility, convenience, and cost effectiveness. Further, as mobile payments have grown into the mainstream, consumers have shown that they want to use mobile devices to access traditional financial mechanisms such as bank accounts and credit cards, financial management tools, and new payment methods such as prepaid cards, digital wallet balances, and digital currencies.

Having these capabilities allows consumers and merchants to engage in transactions more quickly and with less risk. Samsung Pay leverages existing infrastructure and supports all payment terminal types, including magnetic stripe, NFC, and EMV terminals. This means merchants do not have to upgrade or buy additional equipment to support competing mobile wallets. It also increases checkout speed – the consumer just taps their phone to the merchant's point of sale terminal and the transaction is complete (and secure). As recognized by the Federal Reserve System, the U.S. payments system is improved with "ubiquitous, safe, faster electronic solution(s) for making a broad variety of business and personal payments, supported by a flexible and cost-effective means for payment clearing and settlement groups to settle their positions rapidly and with finality."[3]

2. Mobile Payments are Safe and Secure

At the same time, the payments industry recognizes the importance of developing secure and safe payment technologies that protect consumers and businesses from fraud. ETA and its members have been at the forefront in pushing for the development of mobile payment technology that incorporates advanced security technology.

How safe is paying with a mobile device? The answer: about as safe as it gets. Most mobile payment platforms are packed with a whole suite of security solutions which, layered together, make a smartphone nearly impenetrable to fraud or theft.

Mobile transactions offer consumers and merchants heightened security through the use of multiple authentication layers, each of which alone can be more secure than a traditional plastic card with an unencrypted magnetic stripe.[4] ETA members, for example, are deploying multiple layers of protection, including tokenization, encryption, biometrics, and other payments technologies that secure systems against criminal intrusions and protect consumers and

[3] Federal Reserve System, Strategies for Improving the U.S. Payment System at 3, released January 26, 2015.
[4] *See* Better Security Through Mobile – "The One-Two Punch" Industry Best Practices, Presented by The Processor Council of the Electronic Transactions Association at 7, released June 2, 2014.

ETA
ELECTRONIC TRANSACTIONS ASSOCIATION
1101 16th Street NW
Suite 402
Washington, DC 20036
www.electran.org
t 800.695.5509
202.828.2635
f 202.828.2639

merchants. These technological capabilities for payments via a smartphone offer multiple verification layers at the point of sale to authorize the payment. The ETA has released an industry white paper to advance the deployment of mobile wallets through industry best practices designed to ensure that mobile payment transactions provide for heightened and robust levels of security and serve as a reliable means for payment transactions.[5]

In particular, most mobile payment systems, like Apple Pay, Android Pay, and Samsung Pay, rely on Near Field Communication (NFC), which is the wireless form of the "smart" EMV chip cards that banks are issuing to their customers. Every time an EMV card or NFC wallet is used to pay for a transaction, the system will transmit a one-time code that is unique to the transaction. Even if the card is counterfeited or the data is intercepted, it can't be used to make a payment, because that one-time code is now worthless.

NFC mobile wallets work in much the same way, with an added step: instead of transmitting the cardholder's account number, the device will send a string of letters and numbers – known as a "token" – that represents the account number (and can only be interpreted by the financial institution receiving the transaction data). This process is known as tokenization, and it represents a huge leap in payments security. Samsung Pay, for example, provides security for consumers and merchants through tokenization and fingerprint authentication features that limit fraud and reduce liability.

But that's not all – tokenization is just the beginning of the "layered security" that's making mobile one of the safest ways to pay. Data is encrypted while it's in transit from the mobile device to whoever is approving the transaction on the other end. End-to-end encryption makes it even harder for thieves to intercept the transaction – but even if they do, tokenization and NFC capability make the data they find totally useless. In this way, a company like PayPal processes payments without revealing financial account information to the merchant. When you choose to pay with PayPal, you provide the merchant only your name, email address, and shipping address (for physical goods transactions). The rest of the payment information is encrypted.

Finally, the industry is continuing to innovate; new biometric forms of user authentication hit the market nearly every day. A number of mobile payment systems incorporate fingerprinting, facial recognition, and a host of other technologies to make sure that no one but the owner of the phone can get into the financial account.

In sum, mobile payments are actively employing new security technology that improves on legacy systems. Mobile devices provide enhanced security, including passcode protection for the phone, biometrics security features like a fingerprint, secure chip technology, geo-locational information to assist with verification, as well as both device and cloud based encryption and tokenization capabilities. These new means to secure payment transactions are enabled by mobile solutions and do not exist in the traditional plastic card ecosystem.[6]

3. Mobile Payments Can Help Increase Financial Inclusion

[5] http://www.electran.org/mobile-payments/
[6] Id. at 8

ETA
ELECTRONIC TRANSACTIONS ASSOCIATION
1101 16th Street NW
Suite 402
Washington DC 20036
www.electran.org
800.695.5509
202.828.2635
202.828.2639

In addition to providing safe, cost-effective, convenient, and innovative payment options for millions of consumers, mobile payments have the potential to provide lower-income or unbanked consumers access to convenient and affordable payment tools and financial services. This is an important goal for ETA and its members. The Board of Governors of the Federal Reserve recognized the potential benefits resulting from increased mobile phone usage, asserting "[t]he relatively high prevalence of mobile phone and smartphone use among younger generations, minorities, and those with low levels of income – groups that are prone to be unbanked or underbanked – makes mobile phones a potential platform for expanding financial access and inclusion."[7]

4. Mobile Payments Support Small Business Growth

Finally, ETA and its member companies are leading the development of services and products that help small businesses accept mobile payments and better compete in the modern retail economy. The development of new payment technology allows businesses to improve the payments experience of their customers through enhanced speed, convenience, efficiency, and multichannel accessibility. This convenience has resulted in the significant and rapidly increasing adoption of mobile payments by both merchants and consumers. Out of the 4 billion transactions PayPal processed last year, 1 billion were made on a mobile device. This growth is continuing – in the most recent quarter of this year, PayPal processed 345 million mobile payments, up 38% year over year. Mobile payments are becoming a key payment technology of choice for people across the world, and in turn, a key driver of economic growth and business activity.

CONCLUSION

The mobile payments space is dynamic and innovative, and consumers and businesses are benefitting from a range of secure, convenient, and rewarding mobile payment options in the marketplace. As mobile payments continue to grow, we hope the government continues to provide a flexible regulatory structure that supports innovation and allows mobile payments to reach its full potential. Mobile payments has the ability to promote fast, secure payments, strengthen information security, and cultivate long-lasting relationships – all of which are important goals for ETA's members.

As the trade association of the payments industry, ETA looks forward to assisting the Committee in its efforts to ensure that merchants, consumers, and the economy continue to benefit from the safety and security of our nation's payments systems.

---

[7] Board of Governors of the Federal Reserve System: Consumers and Mobile Financial Services 2014 pg. 4 (March 2014) http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201403.pdf. Similarly, the Federal Deposit Insurance Corporation has stated that mobile banking "is poised to have the largest impact for the underbanked through its ability to meet day-to-day financial service needs. The anytime, anyplace, and actionable nature of [mobile banking] offers the potential to enhance sustainability of banking relationships." Federal Deposit Insurance Corporation: Assessing the Economic Inclusion Potential of Mobile Financial Services pg. 4 (April 23, 2014) https://www.fdic.gov/consumers/community/mobile/Mobile-Financial-Services-andEconomic-Inclusion-04-23-2014revised.pdf.

STATEMENT FOR THE RECORD

OF THE

NATIONAL ASSOCIATION OF CONVENIENCE STORES

AND THE

SOCIETY OF INDEPENDENT GASOLINE MARKETERS OF AMERICA

FOR THE

HEARING OF THE HOUSE ENERGY AND COMMERCE SUBCOMMITTEE ONCOMMERCE, MANUFACTURING, AND TRADE

DECEMBER 1, 2015

"THE DISRUPTER SERIES: MOBILE PAYMENTS"

This statement is submitted on behalf of the National Association of Convenience Stores (NACS) and the Society of Independent Gasoline Marketers of America (SIGMA). We appreciate this opportunity to present our views regarding the mobile payments marketplace.

NACS is an international trade association representing more than 2,200 retail and 1,800 supplier company members in the convenience and petroleum retailing industry. NACS member companies do business in nearly 50 countries worldwide, with the majority of members based in the United States. In 2014, the industry employed more than two million workers and generated $696.1 billion in total sales, representing approximately 4.0 percent of the United States' GDP– or one of every 25 dollars spent.

SIGMA represents a diverse membership of approximately 260 independent chain retailers and marketers of motor fuel that sell more than 50 percent of the motor fuel sold in the United States. Most SIGMA members are involved in gasoline retailing, approximately two-thirds are involved in wholesaling, 36 percent transport product, 25 percent have bulk plant operations, and 15 percent operate terminals. Member retail outlets come in many forms, including travel plazas, traditional "gas stations," convenience stores with gas pumps, cardlocks, and unattended public fueling locations. Some members sell gasoline over the Internet and a few are leaders in mobile refueling.

Despite the fact that our members' channel of trade conducts more than 160 million transactions per day, we are an industry of small businesses. Less than five percent of the retail motor fuel outlets in the United States are owned or operated by integrated oil companies. The vast majority of branded outlets are locally owned and more than 70 percent of retail motor fuel and/or convenience store companies operate ten stores or less. In fact, more than 60 percent of businesses that sell motor fuels at retail operate just one store.

Mobile payments offer a unique avenue and opportunity to disrupt many problems and inefficiencies in the current payments marketplace. Today's payments ecosystem, which is dominated by Visa and MasterCard is inefficient, opaque, and excessively costly. This is not surprising. Insulated from competition, the card networks have stifled innovation and have had no incentive to innovate or make the system more efficient. Our system is way behind where it should be. Nowhere is this more evident than the fact that the U.S. has only recently begun to transition away from fraud-prone magnetic stripe cards, twenty years after much of the rest of the world began this transition. The mobile payments market has the potential to be an open, transparent, and competitive environment that creates a level playing field for all players. Without proper oversight from policymakers, however, it is possible that Visa and MasterCard will leverage the market power and antitrust problems they have used to dominate payment cards into a dominant position in mobile payments. If that occurs, it risks stifling innovative new competitors and reducing the options of U.S. consumers long into the future. Thus, we encourage lawmakers to closely monitor developments in this field to ensure that innovators have the opportunity to flourish in the mobile payments space so that the best new technologies have a chance to win and consumers have the chance to benefit from that innovation.

I. The current payments ecosystem is not competitive or efficient and has stifled innovation.

The current payment cards ecosystem is marked by inefficiencies that are the direct result of an anti-competitive environment. Visa and MasterCard, which, along with the major banks, pushed electronic banking and the use of payments cards beginning in the late 1970s dominate the payment card marketplace. In fact, the monopolistic nature of the payment card market has stifled innovation. The card networks are insulated from competition and have no incentive to innovate and make the system more efficient.

A. Costs and rules underlying the payment card market have promoted inefficiency.

The lack of competition in the payment card space has disincentivized the adoption of effective data security standards and has imposed unnecessarily high fraud costs on merchants. Despite retailers spending over $6.5 billion each year trying to protect against card fraud, fraud rates continue to rise in the United States because of our long-time reliance on outdated payment card technology.[1] Merchants pay the brunt of those costs.[2]

The Payment Card Industry (PCI) Data Security Standards Council, which is run by the card networks, has established requirements regarding the security of credit and debit card transaction data that retailers must implement. Generally, these requirements cost retailers tens of thousands of dollars per location, and do not ultimately lead to secure systems. Moreover, these requirements do not provide the retailer with any liability protection in the event data is breached and stolen. Despite banks' false claims that they provide merchants with a "payment guarantee," merchants are constantly hit with "chargebacks." These chargebacks are the euphemism the payment industry uses when they do not give the merchant any of the purchase price on a fraudulent payment card transaction. In other words, for charged back transactions, the merchant absorbs the full cost of the fraud.

The card networks' market dominance has given them the power to force retailers to comply with second-rate security that preserves the networks' marketplace advantage. Under the card companies' operating rules, for example, retailers are prohibited from requiring customers to enter a PIN when accepting debit cards. This is astounding, since PIN authentication is *six times more secure* than signature authentication.[3] It is not, however, surprising. By prohibiting

---

[1] The card networks finally mandated a transition to "chip" cards that went into effect on October 1, 2015. However, these EMV cards are already old technology—Europe has been using "chip-and-PIN" cards since the 1990s.

[2] According to an annual report by LexisNexis and Javelin Strategy & Research on the "True Cost of Fraud," in 2009, retailers suffered fraud losses 10 times higher than financial institutions. The report found that half of retailers' fraud losses came from unauthorized transactions and card chargebacks. The 2013 report found that merchants are "paying more per dollar of fraud than in 2012, the most since 2010." And according to the most recent data from the 2015 report, merchants incur a $223 loss for every $100 of fraud losses. *See* https://www.lexisnexis.com/risk/insights/true-cost-fraud-infographic.aspx. In addition, card-issuer losses are dwarfed by merchant fraud losses, which the Mercator report has estimated to be tens of billions of dollars a year. *Cited in* "House of Cards: Why your accounts are vulnerable to thieves," Consumer Reports, June 2011.

[3] Federal Reserve Board, Debit Card Interchange Fees and Routing, 77 Fed. Reg. at 46,261 (Aug. 3, 2010), *available at* http://www.gpo.gov/fdsys/pkg/FR-2012-08-03/pdf/2012-18726.pdf.

PIN authentication, Visa and MasterCard are able to drive traffic to their signature networks where they are able to collect much higher swipe fees. This is also what has motivated the card companies to push "Chip-without-PIN" in the United States rather than "Chip-and-PIN," which they have used in other parts of the world.[4] And, of course, when banks act like merchants by accepting payment cards for something of value (cash) at ATMs, those banks universally require the use of PINs. The card networks do not interfere with banks' security at ATMs. Unfortunately, they do interfere with merchants' efforts to require PIN entry.

Focused on profits and insulated from competition, the card networks have no reason to improve efficiency, cut costs, and enhance security. They make more money with the status quo. Thus, merchants remain at the mercy of the card companies' policies, which, as we are seeing with the EMV transition, are not designed to maximize consumer protection, card transaction security, or efficiency.

B. The payment cards marketplace is opaque and rife with exorbitant costs that have negatively impacted consumers and merchants.

The dominant card networks set the swipe fees that the banks that issue payment cards charge merchants each time a merchant accepts a card. These swipe fees have grown dramatically over time as Visa and MasterCard have increased their stranglehold on the market. Because these fees are centrally set, banks which should be competing against each other agree to charge the same fees. This results in a significantly over-inflated fee. Despite the fact that banks compete on other business costs – from loan and fee rates to consumers' checking account interest – they do not compete on swipe fees. As a result of this price-fixing and Visa and MasterCard's market power, there has been no meaningful competition to push swipe fee costs down. Rather, the system encourages and perpetuates inflated swipe fee revenue that has enabled issuers to collect excessive profits well above what it would take to cover card program costs.

Not surprisingly, swipe fees have been increasing at an alarming rate. In the last fifteen years, the fees have increased from $12 billion to over $60 billion per year. This has made swipe fees the fastest-growing cost retailers in the United States have. In fact, the average U.S. swipe fee (more than 2%) is the highest of any industrialized country.[5] For most retailers, swipe fees are their second highest operating cost – less than labor but more than items like rent and utilities.[6]

---

[4] Visa advertises PIN benefits on its own website, noting that in the United Kingdom, fraud related to lost and stolen payment cards has decreased by more than half since chip-and-PIN was adopted there in 2004. *See The Benefits of Chip and PIN for Merchants, available at* http://www.visa.ca/chip/merchants/benefitsofchippin/index.jsp (last visited Nov. 25, 2015). Similarly, in their 2013 petition to the Australian Competition and Consumer Commission for authorization to *require* PIN authentication on transactions involving their cards, Visa and MasterCard made numerous pro-PIN statements, including: *"The Applicants' view is that chip and PIN is a significantly more secure form of [customer verification method] than signature." See generally*, Visa & MasterCard – Authorisations – A91379 & A91380, *available at* http://registers.accc.gov.au/content/index.phtml?itemId=1120516.

[5] According to the Nilson Report, the U.S. spends more on swipe fees than the rest of the world combined.

[6] The convenience store industry paid over $11 billion in swipe fees last year. *See* NACS, State of the Industry Annual Report for 2014.

Problematically, most companies have no way to plan for or deal with rising swipe fees. While businesses can make cost-cutting decisions, including changing suppliers or installing more energy-efficient equipment, they cannot do the same when it comes to swipe fees. Thousands of banks such as Bank of America, Wells Fargo, Chase and others that operate under either the Visa or MasterCard umbrella charge precisely the same schedule of fees. There is no price competition to push the price down. Companies do not know when or by how much fees will increase—and because the card networks have made swipe fee rate schedules more and more complex, even after a new rate is announced, it is nearly impossible to understand how those rates will impact a merchant's fees. These uncontrollable and unpredictable costs have a far-reaching negative impact, not only do they lead to higher costs for consumers, they prevent merchants from hiring new employees and opening new locations.

II. Mobile payments innovation presents a unique opportunity to disrupt and overcome problems in the current payments marketplace.

Innovation in mobile commerce has the potential to address the inefficiencies that currently plague the U.S. payments marketplace. To succeed as a "disruptive technology," however, mobile payments must be truly innovative in how they process and effectuate transactions. Just transferring the current payment cards system onto a cell phone is not innovation. This, for example, is the reason that merchants were not particularly enthusiastic when Apple came out with its mobile payments platform. Apple Pay is not truly innovative because it merely links existing credit- or debit-card accounts to mobile phones—it does not actually address the payment system's fundamental problems. Other than allowing consumers to leave their wallets at home, Apply Pay does not provide consumers (or merchants) with added value.

Mobile technologies like Apple Pay that simply graft existing payment cards miss the opportunity to change the economics of payments. If extra, anti-competitive costs are taken out of payments, consumers and merchants can reap the benefits. That would spur economic activity and efficiency.

For a payment technology to be truly innovative and disruptive, it must actually take costs out of the current payment ecosystem and make transactions more efficient. When paper money was invented, it disrupted a traditional system of barter and trade precisely because it made it cheaper and faster to purchase goods. Mobile payments innovations can and should do the same. A classic example of a wildly successful and disruptive mobile technology is the Starbucks App. The App saves Starbucks money that it was paying in swipe fees. To incentivize its use, Starbucks gives its customers large discounts on purchases. That has resulted in a large, loyal group of users of the Starbucks App, has saved users money and has saved Starbucks money. That is a win all the way around. And, by they way, it is by far the most used and most successful mobile payments system in the nation.

In order to achieve similar success to the Starbucks App, mobile payments innovation must be driven and shaped by true competition that consistently encourages greater efficiency.

The rules underlying any particular mobile payments technology must be transparent so that consumers and merchants understand the costs involved and can make informed business decisions.

III. Policymakers have an important role to play in the nascent mobile payments space.

Mobile payments present a unique opportunity to resolve serious problems in the U.S. payments ecosystem and enhance U.S. dominance in the payments field. Innovation properly grounded in competition will enhance efficiency, lower transaction costs, and lead to stronger consumer protection and security. Merchants remain concerned, however, that without lawmaker vigilance, Visa and MasterCard may move their dominance in payment cards into the mobile space and stifle innovation.

One potential example of Visa and MasterCard abusing their market position may be occurring right before our eyes. Merchants are being pushed by the threat of more fraud liability to use EMV card readers in their stores. EMV is a technology that is proprietary to MasterCard and Visa. And, those two card networks have been engaged in a campaign to ensure that the near field communication (NFC) technology in those card readers is turned on. The mobile payments technologies that use Visa and MasterCard products (like Apple Pay) rely on NFC technology. There are, however, many other technologies that are being used and developed by competitors. In England, Visa has just announced they will require merchants to accept NFC payments. This is the type of antitrust violation, referred to as "tying," that American merchants fear. If Visa and MasterCard require the acceptance of their mobile payments technology for a merchant to be able to accept their traditional payment cards, then they may kill-off the other innovators trying to get a foothold in the mobile payments world. This Committee should not allow that to happen.

* * *

Merchants, including our members in the convenience store industry, are extremely excited by mobile technology's "disruptive" potential. But we are also very nervous that the incredible innovation we anticipate could be squashed by the currently dominant payment networks. Therefore, we ask lawmakers to closely monitor the major players in the payments ecosystem to ensure that they are prevented from using market power to dominate this nascent field.



Statement of the

National Retail Federation

submitted to the

United States House of Representatives
Committee on the Energy and Commerce
Subcommittee on Commerce, Manufacturing and Trade

for its hearing

"The Disrupter Series: Mobile Payments"

held on

December 1, 2015

David French
Senior Vice President,
Government Relations

On behalf of:

National Retail Federation
1101 New York Avenue, N.W., Suite 1200
Washington, D.C. 20004
(202) 783 –7971
www.nrf.com

Introduction

Chairman Burgess, Ranking Member Schakowsky, and Members of the House Energy and Commerce Subcommittee on Commerce, Manufacturing and Trade: On behalf of the National Retail Federation (NRF), I appreciate the opportunity to submit this written statement to the Subcommittee in connection with its hearing, "The Disrupter Series: Mobile Payments," held on December 1, 2015.

NRF is the world's largest retail trade association, representing retailers of all types and sizes, including discount and department stores; home goods and specialty stores; Main Street merchants; grocers; wholesalers; chain restaurants; and Internet retailers from the United States and more than 45 countries abroad. Retail is the nation's largest private sector employer, operating more than 3.6 million U.S. establishments and supporting one in four U.S. jobs and 42 million working Americans. Contributing $2.6 trillion to annual GDP, retail is a daily barometer for the nation's economy. Retailers create opportunities for life-long careers, strengthen communities at home and abroad, and play a leading role in driving innovation. NRF's *This is Retail* campaign highlights the industry's opportunities for life-long careers, how retailers strengthen communities, and the critical role that retail plays in driving innovation.

Customer service is at the heart of a retailer's business. Moreover, it is the key to sustaining business growth in a highly competitive industry. Every day retailers must compete to keep customers in a world where loyalty is being awarded to the retailer who provides the best shopping experience through pricing, personalization and convenience. To win and maintain customer relationships, retailers must earn customers' trust by providing value and convenience. Trends and revolutions within the retail industry, such as the rise of e-commerce and m-commerce, mean that implementing emerging and disruptive technologies not only creates efficiency and complements traditional business practices, but also enhances the customer experience. Technology increases expectations for shoppers and raises standards for shopkeepers, and the retail industry continues to embrace opportunities for growth – in innovation, customer satisfaction, and bottom lines. One such opportunity is the advent of mobile payments. Change is forcing a better customer experience.

There is no one agreed definition for mobile payments. Payments made from a laptop using traditional payment methods, such as credit cards, are deemed by some to be 'mobile,' as are point-of-sale (POS) payments in which a card embedded with Near-field Communications (NFC) is used to complete a transaction in the traditional manner. In our view, these are simply existing payments communicating with a different modality. For rough simplicity, mobile payments, also referred to as mobile money and mobile wallet, are payments where a mobile device is used to conduct a POS transaction. The use of in-store mobile payments is effecting change in the marketplace, and this disruption is shaping how retailers and customers behave and interact with each other, as well as with many other entities. In addition to merchants and consumers, the mobile payments ecosystem includes software developers, hardware manufacturers, application developers, data brokers, loyalty program administrators, payment

card networks and processors, financial institutions, advertising companies, and telecommunication providers, to name a few. The development and implementation of mobile payments and related products and services has the potential to provide great benefits to retailers and customers alike. For retailers, chief among these benefits is the prospect of providing customers with a better overall transaction experience due to improvements in transparency and competition; convenience and speed; and security.

Competition

Market competition and transparency are important factors that dictate the quality of customer service a retailer is able to provide. Mobile payments are poised to disrupt competition among payment methods and between the providers and developers of those methods. Right now, traditional payments methods are imposed on merchants by a consortium of card companies and banks who have, for many years, collectively exerted near monopoly power over the business community. Although the relationship between those powerful institutions and retailers is purely contractual, it has become essentially compulsory in practice because each retailer is subject to their substantial combined market power. The exercise of monopoly power by traditional payment providers has led to increased prices for services. With mobile devices functioning as POS terminals, however, customers now have more choices than ever in how to pay. Preserving an open and competitive environment for the development of mobile payment options is essential for retailers and our customers.

Innovation in payment technology moves American consumers beyond the traditional methods of cash, check, and credit card – from payments-embedded apps to text messages to direct ACH payments. Considering the growing number of mobile-friendly payments methods available to American consumers on their mobile devices, there is a new saying in retail that is particularly appropriate in this context: "Competition is only one click away." The more competition there is for faster, easier and more secure payments, the more useful innovation we will see flourish. Likewise, advancements in innovation will lead to greater competition. Together, innovation and competition will help customer adoption of new payment methods.

Convenience and Speed

Customers want to complete their transactions quickly and easily, and retailers are eager to oblige by utilizing technology to streamline and simplify the shopping experience. Mobile payments solutions offer convenience and speed that traditional forms of payments do not always offer. Mobile payments have the advantage due to their inherent portability, flexibility, speed, and ease of use.

A single mobile device that allows consumers to complete transactions and build loyalty is more portable and convenient than carrying around a wallet with cash, various debit and credit cards, rewards and gift cards, coupons, and loose change. The customer may choose which method of payment she would like to use, from an app or a tap of her phone, without being

restricted to the items in her wallet; and a savvy retailer may want to instantly serve discounts or incentives to encourage a customer to choose the most cost-efficient or secure option in her mobile wallet.

History has shown us that consumers adopt new technology if it provides value and adds benefit to them. Loyalty rewards incorporated into new mobile payment platforms are another complement to speed and choice. Customers have shown they enjoy building loyalty through the adoption rate of the Starbucks App, among other emerging mobile payment platforms. Starbucks also sees the benefits of their mobile app through increased customer loyalty and lower transaction fees. Convenience, speed and flexibility are critical to consumer adoption of a new payment platform.

Opportunity for Increased Security

As technology to process mobile transactions continues to evolve at a rapid pace, technological advancements in data security do as well. Mobile payment technology allows for emerging security solutions such as tokenization, encryption, and multifactor authentication, whereas traditional payment systems temporarily store or transmit data in an unencrypted form. While these new security solutions embedded within a mobile device make great strides in preventing fraudulent transactions, mobile payments are additionally secure thanks to everyday precautions such as password protection. Owners of mobile devices can not only set a password to gain entry to the device itself, but can also set passwords or use other authentication methods to gain entry into each and every downloaded app, stored credit card, or linked account.

The retailer-customer relationship is fueled by the sharing of information between merchants and their customers. Among other things, the data collected by retailers ensures the right merchandise is stocked on shelves, customers are offered the best sales and promotions, and stores are opened in locations where demand is the highest. To sustain this trusted relationship, it is imperative to protect this information to provide the best experience. One scenario cannot exist without the other, and protecting customers' data remains a top priority for retailers. Disruption in the payments ecosystem allows for security enhancements that will complement tools retailers currently utilize.

Conclusion

While there are still a lot of questions surrounding the implementation and use of mobile payments, this area of innovation has the potential to provide benefits for both customers and merchants. As long as these benefits continue to support the prospect of an improved shopping experience for our customers through increased competition and transparency, convenience and speed, and securely protect their data, NRF will remain enthusiastic and optimistic about mobile payments technology.

NRF thanks the Subcommittee for their educational hearing on disruption and mobile payments and looks forward to working with Members of the Subcommittee as it continues to monitor this issue.

FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

December 16, 2015

Mr. John Muller
Vice President for Global Payments Policy
PayPal, Inc.
1250 I Street, N.W., Suite 1202
Washington, DC 20005

Dear Mr. Muller,

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Tuesday, December 1, 2015, to testify at the hearing entitled "The Disrupter Series: Mobile Payments."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Wednesday, December 30, 2015. Your responses should be mailed to Dylan Vorbach, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to **Dylan.Vorbach@mail.house.gov**.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Michael C. Burgess, M.D.
Chairman
Subcommittee on Commerce,
Manufacturing, and Trade

cc: Jan Schakowsky, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade

Attachment

PayPal, Inc. Response to Rep. Cardenas' Questions for the Record
Hearing before the U.S. House Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade
"Disrupter Series: Mobile Payments"
December 1, 2015

1. What happens if a transaction doesn't go through – for instance, if the consumer uses a mobile device to pay at a parking meter and the payment doesn't go through for some reason, what is the consumer's recourse for the resulting ticket?

The consumer protection for mobile payment methods is the same whether a transaction takes place by mobile device, by a non-mobile computer, or by plastic card. PayPal provides additional consumer protection measures, along with real-time notification when a transaction is completed.

Mobile devices are just a communication channel for existing payment methods, which include credit cards, debit cards, prepaid cards, direct debit to a bank account (ACH) and mobile billing. (I should note that despite the use of the term "mobile" billing, this can be used for purchases on a non-mobile computer from the limited number of merchants who accept this method, or possibly even in person).

The consumer protections required by law are different depending on payment method facilitated by a mobile device, with credit cards having the most protection, and mobile billing having the least clear consumer protection. Further, these differences have existed for many years, long before the popularity of smart phones.

However, programs such as PayPal Buyer Protection have made those differences less meaningful, since we offer the same purchase protection regardless of payment method.

In response to your specific example, the advantages of mobile devices are the real-time notification. The customer will get a notice if the transaction went through, so if they don't get a notice they can assume something went wrong (and of course, if available, they can also look at the parking meter to check that they were credited with the right amount of time).

2. What if a consumer is charged the wrong amount?

If a consumer is charged the wrong amount, she has Error Resolution rights that are essentially the same for credit cards, debit cards, and ACH under Regulation E and Regulation Z. This means that the consumer is entitled to [explain]. Furthermore, these Error Resolution rights are the same whether the transaction is initiated by a mobile device, a credit card, written instruction to the merchant, or any other access device. The device on which the consumer makes the purchase does not change their rights under existing law.

3. Currently credit cards charge merchants a fee for the transaction. How will fees be determined with mobile pay? Who pays the fee in a charitable giving situation?

In most cases, including at PayPal, the fees to the merchant for a mobile payment are the same as the fees for any other E-commerce or Card Not Present payment. Other services may charge an extra fee to the bank, but not to the merchant. For donations to charities, many merchant processors (including PayPal) have a special reduced rate for registered 501(c)(3) charities. The charity, not the donor, pays the fee but some charities ask donors to "top up" their donation to cover payment processing and other overhead costs.

FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225-2927
Minority (202) 225-3641

December 16, 2015

Ms. Jessica Deckinger
Chief Marketing Officer
Merchant Customer Exchange
21 Hickory Drive, 3rd Floor
Waltham, MA 02451

Dear Ms. Deckinger,

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Tuesday, December 1, 2015, to testify at the hearing entitled "The Disrupter Series: Mobile Payments."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Wednesday, December 30, 2015. Your responses should be mailed to Dylan Vorbach, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to **Dylan.Vorbach@mail.house.gov**.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Michael C. Burgess, M.D.
Chairman
Subcommittee on Commerce,
Manufacturing, and Trade

cc: Jan Schakowsky, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade

Attachment

Additional Questions for the Record
Formal Response Provided by Jessica E. Deckinger
December 23, 2015

Honorable Tony Cardenas

(1) Can you speak to the customer experience in your Columbus pilot? What are you learning?

CurrentC's public beta in Columbus has been hugely valuable to MCX as we continue our effort to build a mobile payment app that offers consumers choices and convenience at checkout. Consumers have participated in the Columbus beta at over 200 locations, including at retailers, restaurants, and fueling stations. MCX has learned, through the beta, that consumers care about ease of use, convenience, security and value from mobile wallets. These insights are vital to our preparations for our national launch. They are being used to refine our product road map, improve user experience and enhance the app's functionality.

(2) Many consider mobile payments the most secure form of payment, but with the increase of cybersecurity threats, how can customers be assured that their financial information isn't at risk?

At MCX, we believe it is incumbent on mobile payments technologies like ours not only to use the latest security technology, but to help educate consumers about how it is working for them. We are leveraging cloud technology to avoid storage of any sensitive consumer information on the phone or transfer of such information at POS. Our app uses secure dynamic tokens, uniquely generated for each individual transaction, to facilitate transactions instead of constantly passing the data between the consumer, merchant and financial institution. In the simplest terms, using a "dynamic token" means that consumers can feel assured that their personal financial information or payment information is never stored on the device, is never stored on the merchant POS, and even if the dynamic token were to be stolen, it is worthless because it cannot ever be used again.

(1) Our registration process includes several security questions which are used as identifiers should consumers get "locked out" of the app.

(2) Consumers are asked to create and use a customized 4-digit personal PIN to unlock the app every time they exit and re-open it. A lost or misplaced phone can't be used to pay under normal circumstances, because the 4 digit personal PIN needs to be activated for each and every payment transaction.

(3) We provide an easy to follow process to disable a phone from CurrentC should a consumer lose her mobile device and wish to shut her account down for peace of mind.

FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

December 16, 2015

Ms. Sarah Jane Hughes
University Scholar and Fellow in Commercial Law
Maurer School of Law
Indiana University
Bauer Hall 266
211 South Indiana Avenue
Bloomington, IN 47405

Dear Ms. Hughes,

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Tuesday, December 1, 2015, to testify at the hearing entitled "The Disrupter Series: Mobile Payments."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Wednesday, December 30, 2015. Your responses should be mailed to Dylan Vorbach, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to **Dylan.Vorbach@mail.house.gov**.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Michael C. Burgess, M.D.
Chairman
Subcommittee on Commerce,
Manufacturing, and Trade

cc: Jan Schakowsky, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade

Attachment

Sarah Jane Hughes
Responses to Additional Questions for the Record
Posed by the Honorable Tony Cárdenas
"The Disrupter Series: Mobile Payments"
December 1, 2015

Question 1 from Representative Cárdenas: How do mobile payments assist unbanked and under-banked individuals? Is this at a lower cost than other options available?

Question 2 from Representative Cárdenas: How do mobile payments help small businesses?

Question 3 from Representative Cárdenas: What do you see as the biggest obstacle to mobile payment adoption? What can be done to fix it?

***

Question 1 from Representative Cárdenas: How do mobile payments assist unbanked and under-banked individuals? Is this at a lower cost than other options available?

Response from Sarah Jane Hughes:

"Representative Cárdenas, Mobile payments assist unbanked and under-banked individuals in numerous ways. It is important to recognize that the manner in which mobile payments assist each group may be different so I have organized my response by looking first at special values to both groups and then at special values to one or the other of these groups.

Before beginning my direct answer, I would like to distinguish between "mobile payments" and "mobile banking." A mobile payment may not require the consumer who owns the mobile phone to access a bank account. Thus, a consumer can make a deposit of funds to a merchant such as Starbuck's and then debit purchases from that deposit via the mobile phone. This type of transaction is conceptually comparable to that consumer using a prepaid card that she purchased from Starbuck's. Of course, that deposit only works at Starbuck's so its utility is limited compared with other options.

A second category of mobile payments do not require advance deposits of funds. Rather, the consumer authorizes a payment that gets billed to the consumer's mobile phone service account in the following month. This type of "mobile payment" does not fall under the Electronic Funds Transfer Act or Regulation E because there is no underlying "account" at a depository institution from which the payment is debited.

Other "mobile payments" work more like traditional credit or debit cards in that they provide the consumer to access her own demand deposit account at a depository

institution. The phone is the device used to access the demand deposit account – rather than using the card as the access device. The phone operates as a means of storing credentials and also as the link for communicating the consumer's authorization for the payment transaction to be processed by the merchant and along the path to the consumer's own demand deposit account.

"Mobile banking" refers in my view to my communications with the bank that holds my demand deposit account. Unbanked individuals would not have access to "mobile banking." Under-banked individuals would have access and might find communicating with distant branches or banks without branch networks very convenient and reasonably priced.

Now proceeding to your specific question, mobile payments assist both unbanked and under-banked individuals by allowing them a ready alternative to cash or debit and credit transactions at participating merchants. Smart phones – through which most mobile payments are made in the United States – operate as substitutes for home computers for increasingly large numbers of unbanked and under-banked individuals and, thus, allow the consumer access to making payments they otherwise might have to make in person or through more expensive and time-consuming means, such as by procuring money orders or cashier's checks.

Focusing a bit more on the issue of cost, mobile payments can be cost-effective for consumers compared with some optional means for making payments. As noted above, they can be less costly that using money orders or cashier's checks for payments made by consumers who do not have bank accounts. For others, mobile payments and other Internet- or telephone bill payment options can prevent late payments, higher interest charges or default on a credit relationship with an accompanying repossession of a valuable consumer item, such as a car.

However, if a payment issue arises outside the scope of an established legal regime such as the protections of Regulation E and the Electronic Fund Transfer Act, the lack of predictability in the outcome of disputes or resolution of errors can make mobile payments costly for consumers.

Question 2 from Representative Cárdenas: How do mobile payments help small businesses?

Response from Sarah Jane Hughes: Payments innovations that enable more small businesses to engage with more customers are good for the economy. As a means of making payments, mobile payments may become more important to small businesses in several ways. First, as commercial banks shrink their networks of branch banks, using mobile payments and remote deposit capture of checks will reduce the difficulty, time, risk and cost of moving cash or paper payments instruments such as checks from merchants to banks. Second, to the extent that transactions clear and settle faster when made through mobile payments or mobile banking, such a development will aid small

businesses in managing cash flow and save them certain forms of accounting expenses and reconciliation.

Additionally, mobile payments may help merchants capture more impulse transactions than they might have if the consumer has left her cash, checkbook, or credit card at home on the day of the transaction.

Finally, mobile payments allow merchants to reach unbanked and under-banked consumers and, thus, expand the range of customers their businesses can serve.

I should say that to the extent we expect mobile payments to contribute to the general economy and to the prosperity of small businesses, we need to ensure through sound guidance from Congress that functional regulators that depository institutions continue to provide banking services to small businesses no matter where they may be located.

Question 3 from Representative Cárdenas: What do you see as the biggest obstacle to mobile payment adoption? What can be done to fix it?

Response from Sarah Jane Hughes: The lack of more orderly laws governing the data security and privacy rights of individuals among the participants from merchant to payments processors and mobile providers as well as depository institutions is one of the bigger obstacles to wider acceptance, particularly as consumers focus more attention on privacy and data security following the high-profile data-security breaches and identity thefts events of the past four years.

Additionally, the lack of laws spelling out the responsibilities of the mobile service providers is an obstacle because of unfair, deceptive and abusive practices that some mobile service providers have allowed third parties to perpetrate via the providers' monthly statements. These include "mobile cramming" billing problems as I mentioned during my testimony that the Federal Trade Commission, Federal Communications Commission, State Attorneys General, and the Consumer Financial Protection Bureau addressed in federal court and administrative enforcement proceedings over the past two years, and the apparent lack of well-grounded dispute resolution procedures among the mobile service providers to set forth charges on bills in a straightforward manner or to handle consumers' complaints about cramming on their bills.

Congress might revisit the allocation of responsibilities among the FTC, FCC, and CFPB for enforcement of laws pertaining to mobile payments (not mobile banking) and fill in gaps between the existing regulatory schemes and legislation, and engage in oversight to be certain that the agencies are fulfilling Congress' purposes in enacting the laws that govern in this area.

FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115

Majority (202) 225-2927
Minority (202) 225-3641

December 16, 2015

Mr. Sang W. Ahn
Chief Commercial Officer, U.S. Samsung Pay
Samsung, Inc.
30 West 26th Street, 7th Floor
New York, NY 10010

Dear Mr. Ahn,

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Tuesday, December 1, 2015, to testify at the hearing entitled "The Disrupter Series: Mobile Payments."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Wednesday, December 30, 2015. Your responses should be mailed to Dylan Vorbach, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to **Dylan.Vorbach@mail.house.gov**.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Michael C. Burgess, M.D.
Chairman
Subcommittee on Commerce,
Manufacturing, and Trade

cc: Jan Schakowsky, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade

Attachment

Mobile Payments Hearing: Samsung Responses to Questions for the Record

The Honorable Tony Cárdenas

1) A recent study done by the Pew research center shows that 13% of Latino Americans rely on their smartphone for online access compared to 4% of White Americans. Yet, Hispanics display a lower financial literacy level than their White counterparts. What is Samsung doing to educate consumers?

Samsung Pay offers consumers, including our significant number of Hispanic customers, the ability to make secure transactions almost anywhere you can swipe or tap your card. Samsung accomplishes this through our combination of Near Field Communication (NFC) and Magnetic Secure Transmission (MST) technology. With Samsung Pay, Hispanic consumers can now have confidence that their payments are secure regardless of whether they are shopping at the big retailer downtown or the mom-and-pop shop around the corner. Samsung is doing substantial outreach – through marketing and social media – to educate Latino Americans and all consumers about this unprecedented security.

2) How is Samsung Mobile keeping consumer's information secure? What consumer information is being stored in the mobile payment app?

Samsung has partnered with key financial institutions to safeguard consumers' personal, transactional, and payment information. Samsung Pay uses tokenization and authentication methods to secure consumer information. Additionally, Samsung's KNOX service constantly monitors suspicious activity within the device to protect from any malicious attacks. If a device is lost or stolen, Samsung offers a free service to remotely lock or erase Samsung Pay. The service also has the ability to locate the device and erase all stored personal information.

Samsung does not store or have access to the payment information added to Samsung Pay. The last four digits of the card number are displayed on the card image in Samsung Pay to help consumers manage their cards. Additionally, Samsung does not – and cannot – monitor user purchases. After a payment is accepted by the issuing bank, the card network may optionally send a notification back to the device that contains details of the accepted transaction. But these details are encrypted in transit.

3) Can mobile pay be used to wire money internationally?

Samsung Pay does not allow consumers to wire money internationally.

4) What if the system crashes? Let's say in the case of an emergency?

Samsung Pay is a feature that rides on top of the larger financial and payments infrastructure, so it is not a "system" that can "crash." That said, consumers may encounter instances where Samsung Pay does not work at a specific merchant. If this happens, the consumer can still pay with cash or their physical payment cards.

○