UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

PAY ON THE GO:
CONSUMERS AND CONTACTLESS PAYMENT
TOWN HALL MEETING

Thursday, July 24, 2008
8:30 a.m. to 5:00 p.m.

University of Washington School of Law
William H. Gates Hall, Room 133
Seattle, Washington
# TABLE OF CONTENTS

1. **Welcoming Remarks**  
   William Covington, Moderator  

3. **Introduction to Contactless Payment:**  
   What Is It and How It Is Used  
   Katie Harrington-McBride, Moderator  

11. **Consumer Understanding and Acceptance of Contactless Payment Technology**  
    Charles Harwood, Moderator  

41. **Contactless Payment Cards**  
    Julie Mayer, Moderator  

92. **Mobile Payment Devices**  
    Kathyrn Ratté, Moderator  

172. **Meeting the Challenges: Strategies and Approaches**  
    William Covington, Moderator
INTRODUCTION AND WELCOMING REMARKS

MS. MAYER: My name is Julie Mayer. I'm with the Federal Trade Commission here in Seattle, and we want to welcome you here to our event, Pay on the Go: Consumers and Contactless Payment, which is being co-hosted by Professor Bill Covington's Clinic on Technology and Public Policy at the University of Washington School of Law.

So we're at this lovely facility that we are able to use today, and without further ado, I'd like to introduce Professor Covington to welcome you all again to this event.

MR. COVINGTON: Thank you, Julie, and welcome to the University of Washington Law School.

Very briefly, the Technology, Law and Public Policy Clinic is aimed at students who are interested in writing legislation, regulations or research papers on high tech or high tech industries.

Our students have looked at things from the regulation of voice-over Internet protocol through digital rights management. In the RFID space, the students have been looking at things such as consumer protection and privacy rights.
Let me just share a few administrative details with you before we get into the work of the day.

First, attendees may be invited from time to time to ask questions of the panels. If you wish to ask a question, please raise your hand for a staff member to bring you a microphone.

Second, our restrooms are located at the top of the hall. You make a short jog to the left and another to the right, and all will be revealed. Coffee will be available at the Burke Museum, which is across the parking lot directly from the law school. Unfortunately, coffee is not allowed in this particular room.

We will be gathering for an informal lunch at McMahon Hall, and we will be gathering right over by the exit sign for those of you who want to join us for the group lunch. For those of you who want to eat on your own, one block over is University Way. We have a number of eateries that are student certified that you will probably find enjoyable. Please turn off your cell phones.

And last, but far from least, this building is totally Wi-Fi'd, which is both a blessing and a curse to those of us who are faculty. So for those of you who wish to access the Internet, you can go to the
University of Washington website. The network ID is Event 0217. That's Event 0217. Now, the challenging part. The password is W8L2+B9N3+Q9M3. Now, I have a number of papers at the place where I am sitting which contains this information. So if you were unable to keep up with this, I am more than glad to provide you with the access information.

So, again, welcome. Thank you for attending. And at this point, I would like to introduce Chuck Harwood, who is the Regional Director of the Federal Trade Commission. Thank you.

MR. HARWOOD: Thank you, Bill. And, again, my name is Chuck Harwood. I am the Director of the Federal Trade Commission office located here in Seattle.

And I want to begin by welcoming all of you to this event, particularly those who traveled some distance. I know some of you have come from quite a ways away. We have a few benefits we can offer you if you made the long trip; one, obviously, is the weather. It's much better than I suspected than most of the places you came from. And I think we are pleased about that, although I can't claim credit for it.

But then, secondly, I hope we can offer you today an informative and useful program and that you'll also have the opportunity to learn too. You'll have
something to learn from it, and hopefully you'll take time to contribute to our program as well, and to ask questions, comments, continue the dialogue during lunch. Feel free to talk to any of us in the halls.

This is really -- the program is really two parts. Part is the formal part that we're in this room. The other part is just the informal dialogue that goes on between panelists and between the panelists and the audience. And that, in some ways, is arguably the most valuable part of this program.

So the concept of contactless technology or smart cards, and there are various terms that are used, it's enticing. It's even seductive in a way. The idea is that you can quickly and easily complete a transaction.

You know, we've all stood in long lines at Starbucks or McDonalds or something and watched that person way down there in the front fumble with their payment and seem to take forever to get their wallet out and get out that change, and then discover that they have to pay with pennies or something like that. And it just takes forever.

And the idea that somehow you can quickly and easily pay for small transactions or maybe even large transactions by just waving a device or even waving your
wallet in front of a reader or tapping a reader is a concept that just sounds wonderful to consumers. It's quicker, it's easier. Moreover, it might provide opportunities for better recordkeeping as far as consumers understand it. It might provide opportunities -- it just simply has some amazing opportunities or benefits.

But the concern is the consumers possibly are being asked to make tradeoffs, and that's part of what we're here to talk about today. What kind of tradeoffs, if any, are consumers being asked to make? Are they being asked to make tradeoffs regarding privacy or security, and do they understand what those tradeoffs are? Do they understand that the technology is different than the kind of technology they might be -- might have used in the past that involve magnetic strips, for example? Do they understand how this new technology works or do they, in fact, even need to understand the intricacies of what RFID is or how radio frequency works.

That's the part of what we analyze today as well; the technology and the tradeoffs and what consumers understand what they're being told.

We're also going to be talking about just some of the ways in which that technology is being used now.
and some of the ways in which it will be used in the future.

The FTC has been studying this issue for a number of years now. We held a conference in Washington, D.C. in 2004 that looked at RFID generally, and then a year later we published a report from that conference.

We followed that up with a really amazing undertaking called Tech-Ade. In 2006, it looked at a variety of technologies and how they were being implemented and used and their effects on the consumer marketplace.

And one of the topics we looked at in Tech-Ade was also RFID, and we also touched on contactless payment.

And through all this what we've seen, even in the last four years, is that the products have changed. They have morphed. They have developed. Some of the things that we talked about in 2004 haven't happened, and, yet, other things have happened. Some of the concerns we had in 2004, you know, they haven't appeared yet. We haven't seen them. And, yet, in other ways, things that we didn't anticipate happening, happened.

So what we've been dealing with, even in the past four years, is this rapidly changing and morphing
technology. And one of the things that we're hoping to hear about more today is try to get a sense of where the direction is, what directions these technologies are going in, because that's important to us at the FTC. It helps us get a better sense of what we need to anticipate as a regulatory agency, as a consumer protection agency and, frankly, as a consumer education agency. A lot of our interest is simply in communicating, educating consumers about their rights and responsibilities.

So we collaborate with law enforcement agencies and with consumer education agencies and with private industry and with NGOs in the United States, but also with similar organizations around the globe.

And as you'll hear later today, we're going to be -- this is part of a longer-term process, this particular workshop, town hall is part of a longer-term process in which we'll be looking at and talking with our colleagues throughout the world about how they're dealing with contactless payment.

So, in fact, today we're going to hear from some folks who have already dealt with the use of contactless payment, smart cards, whatever you want to call them, in other countries. And that information today, I think, will be useful to all of us. It gives
us a sense of how consumers will be using technology, and will also help us understand what might happen here, and it will also give us a sense of what some of the international challenges are, some of the cross border challenges are for us as we deal with these issues.

So our goal for the day, finally, is to hear from experts, to get a sense of the direction these things are going in, to get a sense of what consumers are being asked to do, to get a sense of what consumers are looking for, and to get a sense of how organizations and entities like the FTC, like private NGOs -- or NGOs, I guess that's redundant, NGOs, to get a sense of how entities such as other federal regulatory entities and even state and local agencies should respond to these amazing technological developments. You get a sense of whether they're -- you know, what our role is in this area.

And I look forward to hearing what I expect will be some really amazing comments and input and insights into this process.

And with that, I think we're probably ready to start our first panel. And I understand our first panel is an Introduction to Contactless Payments and will be moderated by Katie Harrington-McBride, and there she is right there. Katie. Thank you.
INTRODUCTION TO CONTACTLESS PAYMENT:

WHAT IT IS AND HOW IT IS USED

MS. HARRINGTON-MCBRIDE: Good morning, everyone. Thank you very much for being here this morning. I think in spite of the delightful weather, there were some -- the vagaries of travel got the better of some of you, including the gentleman to my immediate right, and we're very grateful for those of you who endured long travel delays and who came great distances, for making those sacrifices to be here.

We're looking forward to, as Chuck said, a really informative day, a day in which FTC staff can learn a lot, and those of us in the room can share ideas and information about the state of the art and what, if anything, needs to be done to make sure that consumers are protected in this world where technology is changing fast.

One of the goals for our panel -- in fact, the primary goal is make sure that we're all on the same page. And so this is really a table-setting presentation and probably different from most of the other panels throughout the day because more so than in any other panel, you're going to have some talking heads here.

We're going to have formal presentations.
We're going to get some slides on the board. We're going to make sure that everybody has a sense of the scope of development in the technology, what contactless payment is, what it means, how it works functionally, and where it fits in the larger scheme. We're going to have some contacts provided as well.

So that's our goal and, perhaps, again, less so than in subsequent panels, we're going to -- we're not going to have as much Q and A maybe. Although, feel free, if you do have questions, to raise your hand and we'll try to get somebody out to get you a microphone. Our goal is if we do have questions, it will be at the end of the two presentations, at the end of each of them. And then we may reserve a little bit of time at the end of both to have a little bit of discussion as well. So we'll see how that goes.

And with that, I'd like to introduce the two panelists who are going to be talking with you this morning. I'm delighted to have with us two experts, Randy Vanderhoof, to my immediate right, is the Executive Director of the Smart Card Alliance. Randy is here to represent his organization and tell us a little bit about the background of contactless, where it's been and where it's going.

And then to Randy's right, we have Dan
Littman, who is an economist at the Federal Reserve Bank of Cleveland in their Payments Research Group. Dan is going to provide us the bigger picture, the even bigger picture on where contactless fits into the payment system generally.

So with that, I will turn it over to Randy, who is going to make a presentation. And after his, we can ask him some questions.

MR. VANDERHOOF: Thank you very much, Katie.

So I really appreciate the opportunity here that the FTC has done to try to bring all of the interest about payments evolution together. My role here as the Executive Director of the Smart Card Alliance, which an industry association, focused on raising the awareness and the adoption and the usage of this technology is really to impart some of the information that's available to you as a public resource, both to industry, as well as to consumers and to merchants on how this technology is evolving and how it's changing, and what are the reasons for this technology even being here and being talked about in the first place.

Our organization is made up of over 180 member groups. They represent all of the industry, participants in the payments field, as well as in the
identity and the security field. So we have a rich community of knowledgeable people who understand the technology, who understand the markets and who understand the end users, which are either the consumers, the retailers, the businesses, even our Federal Government in terms of how they apply this technology in their day-to-day lives.

To try to put a context together of why we're here or what we're talking about, this slide kind of just represents in an informal way the transition that the payments industry has experienced over time in terms of both technology advances and testing new applications or approaches to payments.

So when the first card payment -- first card product came out some 30 years ago, it was a revolution. It took time for people to understand it and trust it, to build an infrastructure around it. And today, we know, as consumers, we can't imagine our lives without it.

Well, over time, we've seen different changes being made to the payments infrastructure. We've introduced other technologies than the plastic or magstripe. One ever the really breakthroughs was the Exxon Mobile Speedpass RF-enabled fob as a means to deliver a payment system as the first real model in the
United States of having an alternative delivery system
to execute a credit or debit transaction.

We went through a period of experimentation
with contact chip technology modeling after some of the
advances that have happened outside the U.S., in Europe
and Asia and other places. And then we saw that in the
United States market, based on the rich infrastructure
we have for an online, real-time payment processing
network, we didn't have to reinvent the wheel and go
back to a very strict, secure, intelligent payment card
and device infrastructure, but rather leverage the rails
that have already been set with the online payment
processing networks and utilize changes to the
technology that can coexist on that platform.

And I think what you've seen in the last ten
years has been a number of implementations around that
we're here now to talk about because it's becoming part
of the day-to-day payments landscape.

This chart just kind of gives you a visual
image. On the right side of the chart is just the
traditional payments network. This is a secure payment
communications infrastructure. It's not the Worldwide
Web. It's much more specialized and focused and
operated by the payments industry.

The acquirer's role is how they interface at
the point of sale in gathering that credit card information. Then it's identified by either its branding of MasterCard, Visa, American Express, Discover, Capital, and then routed out through the network to the issuer who issued that individual's card. It's then authenticated, sent back to the merchant terminal with an authentication and the transaction is completed. All this happens in milliseconds.

The left side of the diagram just shows the delivery system for that information, and we're looking at, in the contactless world, not only the traditional card format, but other form factors such as key fob or keychain devices, watches, and even mobile phones in the future.

So having this freedom to change the form factor and the delivery factor is opening up what we call the new contactless way to pay. It's appealed to a segment of the market where speedy convenience at the merchant level is something that's valued and there's strong business drivers to have.

And, typically, those merchants have primarily depended or used cash or checks for payment rather than people pulling out their credit card. So the fast food or convenience stores, the stadiums, vending machines, movie theaters, taxi cabs, what they all have in common
is traditionally these have been heavily cash-oriented merchant chains that are now, because of the speedy convenience factor, are starting to open and to start to use cards as a means of payment as well.

This is of both benefit to the consumers, who carry less cash with them and are often limited to the decisions they make at the point of sale by how much physical cash they have on them, and also it's a benefit to the issuers of the bank cards because they get people to start using their cards more frequently, which is what they want to try to consolidate around their customer base.

So the Smart Card Alliance really represents the stakeholders of the merchants, the card suppliers, the banks, the manufacturers and such, but we really don't represent the consumer. So we wanted to understand what the consumers' attitudes are to all of this technology, and we commissioned a study. In fact, we commissioned two studies in the last two years to try to get the consumers' ideas about what this technology means to them.

The last study we completed was in April of 2008, and we were able to compare that data with the data we generated our initial study in 2006 to see what kind of attitudes have changed. I think some impressive
information came out of that report.

9 percent of the population are contactless payments users now, which is a significant increase of where we were two years ago. People are more knowledgeable now of what contactless payment is. So they're beginning to understand it and make decisions about whether it's right for them or not, but at least they're now knowledgeable enough to make an informed decision.

Also, people that have actually used the technology really like the technology, and this is also something that's really important because people who are constantly inundated with new innovation don't necessarily like the changes that industry puts forth to them, but we're seeing a rapid acceptance and adoption of the technology once people have actually tried it and used it in their day-to-day life.

Safety and security is always one of the top things that you ask consumers about in dealing with anything that has to do with payments. And contactless payments has certainly raised the awareness about what does it mean for payment security.

So we asked a lot of questions about -- both from users of this technology and even people that haven't used it yet what their perceptions were about
the safety of contactless payment.

68 percent of them said they thought that this technology was as secure as their debit/credit card with signature technology. The number of people who cited that safety was their primary concern for not using it actually has declined in the last two years. As people become more informed about it, they're less -- we've answered a lot of their questions.

And the people that are saying we're still not interested in using it are more not interested because they really don't see the value to them personally to have this other form of technology when their cash or their credit/debit cards that they have traditionally used serve their needs.

Also, when we compared how they felt about -- those who did express a concern about payment security, we asked them, well, how does it compare with your concerns about payment security of your other payment products? And not to anyone's surprise, you know, people are concerned about payment security regardless of what their payment medium is. And, in fact, the percentages are right in line with debit, signature debit, checks and contactless.

So I think the important take-away there is that we're never going to have a consumer population
that's totally comfortable and feeling safe and secure about payments, but this technology doesn't raise any significant higher barriers to that concern than any of the other existing products that are on the market.

The reason why contactless has been the fastest adoption of a new payment form factor and process in the experience of the payments industry is because other attempts to introduce advanced payment technologies have usually been driven by benefits to the financial industry in terms of making them more secure, but the penalty was that merchants had to invest more in the payment infrastructure and didn't share in the benefit of the reduced fraud significantly or that consumers really weren't getting anything more from their payment product than they had before, but may have had to change the way in which the product was used or how long it took them to make a transaction.

So what made contactless work was that it really appealed to the three stakeholders with tangible benefits to the issuing banks, to the merchants, and to the consumers.

And without going through all of the bullets there, the highlight for a consumer is, I just want to be able to trust my payment product. I want it to be fast and easy and simple. And if you can make my life
simpler or get me through the lines faster and also allow me to do that transaction and feel safe, then I'm certainly going to be attracted to that.

From the issuer's standpoint, they had something new to present to their customer. So issuers are in a very competitive market. Everybody has multiple card products. They're all fighting for that top position, and they're looking for ways to innovate to be able to offer something more than what somebody else has to offer. And this technology has offered them an opportunity to market a new concept, and also to add additional benefits, and more importantly, to be able to get people to start using their products more and more in their day-to-day lives.

And the retailers, which are the ones that have to invest in the infrastructure to accept contactless payments, rather than trying to drive this through the entire retail chain, what the brands did and the issuers did, which I thought was very bright, is they looked at the target market which would achieve the highest benefit, which was the convenience stores, the fast food locations, et cetera, because they were going to be the folks that would prove whether or not this new payment platform was really going to catch on in the consumer market.
So when we reached out to the consumer -- to the convenience stores, the fast food chains, the movie theaters and such, what they found was that, yeah, not only did this move people through their lines faster, but it also created a better shopping experience for their consumers and, therefore, the consumers started to populate those stores more frequently. They started to use the card in more creative ways and add additional purchases. All of this was a way where retailers could get more traffic through their lines and be able to target some more benefits to their consumers.

Because we have this form factor independence not only at the device level, the card or the key fob or whatever it is that you're carrying, but specifically at the point of sale, at the terminal, the image that you have of the contactless payment terminal is there's a little target device there on the screen, and you hold your payment device to that device, and it reads the information, processing the transaction.

The significance of that is that that's a sealed carrier, unlike the magnetic stripe wedge which has an open slot that has to be kept clean and available for people to read the information off the magnetic stripe.

Because this is simply a closed payment
interaction, it allows for those payment devices to be placed in outside, foul-weather areas with a much higher degree of reliability because they aren't exposed to the challenges of weather or the challenges of an individual that has to orient their payment product to the direction of the swipe, et cetera.

So things like vending machines, which have a very tight space in terms of their display for what they can do to accept coins and bills and possibly cards, by simply integrating the contactless payment technology on to the face of that device, they can now offer another whole payment medium in terms of credit cards and debit cards that they couldn't have supported before because they didn't have the real estate to put a big wedge reader and have a device that would communicate back to the payment processors.

Taxi cabs -- the number of cities -- I live just outside of Philadelphia. Philadelphia is one of the first cities to implement payment with a credit card at a taxi. What a great idea. I mean, how many of us have been riding in taxis and scrambling for money because we didn't have an option of using the card in our wallet. This has been -- you know, consumers love this idea. Taxi drivers aren't so keen on it for other reasons.
There was a pilot with the Ohio Turnpike to use this as a means of payment on the highway. They couldn't accept credit cards at a machine on the highway because, again, the outdoor infrastructure and place and the risks associated with the swipe not being able to be read, the slowness of the transaction, having to sign it and things. But now having this contactless card or key fob device, they can achieve their speed of transaction and reliability of transactions, and it opens up another means of convenience of payment that motorists didn't have available to them before this technology came on board.

The top one there, the New York City Transit Pilot, one of my favorite effects of what contactless payment brings to bear, and that is if you've been in New York City or even any major city and used the mass transit system, the typical process is you go into the system. You go up to a kiosk machine, put your cash or your credit card in the machine. You transfer value on to a transit pass or card, and then you enter the system to use the system. Nine times out of ten, you're probably buying a $5 card and you're using $3.25 cents of it, and the card gets tossed away, et cetera.

What New York City is piloting is by implementing contactless payment at the turnstile.
They're going to bypass that whole line. When people enter the system, rather than going to the kiosk or going to the booth, transferring their payment to a transit pass or transit card, they can now walk right to the turnstile, tap their keychain device or their phone or their card, and it will deduct only the fare for that transaction and they go through the system. So opening up that opportunity, consumers are going to like that. Certainly, the transit operators feel very comfortable as well. So this is the kind of innovation that is spurring with this capability.

I wanted to add one more slide in there just to cover some of the issues about security because I know it's going to be a subject of discussion for the balance of today. And I wanted you to give what the Smart Card Alliance's analysis is, which has been through the contribution of all of the major card brands and the issuers and the technology providers that have validated that this information is, in fact, accurate.

When we talk about contactless payment security, we have to talk about payment security as a whole, and look at payment security in the context of how consumers actually use payment.

Nobody questions the fact that cash is still the most widely-used method of payment, and there's no
security associated with cash. If I lose my wallet or
if I lose the cash out of my pocket, you can't identify
it. So the advantage is it's anonymous. The
disadvantage is that there's no way to tie it to the
individual.

Well, in terms of magstripe cards and debit
cards and credit cards and contactless payment, there's
all going to be different ways in which consumers are
used to using this and feel comfortable using it, and
the option is that people will use this technology at
their level of comfort. There's no one forcing them to
use it in ways that they're not comfortable with and,
therefore, people should make their own informed
decisions about, does this new technology create an
opportunity or a threat for me? Let me understand what
that is, and then I can make those decisions in terms of
how and where and when I use it at my own choice rather
than what somebody else is asking me to do.

So radio frequency is probably the key point
that we tend to circulate back to. This is different
because we've never had a payment product that generated
our account information through a radio frequency
interface to the terminal. It's always been a
deliberate act of a user swiping their card through a
terminal or entering their account number through their
keyboard, and now we're doing this airwave communication.

You need to know that all radio frequency technology is not the same, that there are secure radio frequency technologies. There are insecure, in terms of a spectrum of capabilities. Transit cards are different than bank cards, are different than tags that are on our computers and our office furniture. So we must understand the context of the radio frequency technology as it's applied in this application for contactless payments to make clear decisions about that.

This technology was chosen because it has a very narrow read range. It says ten centimeters, which is about four inches. The actual read range of that is between one and two inches in terms of how the terminals or the readers are programmed to read the tags.

The reason for that is that they wanted this technology to be a deliberate read of somebody having to hold it or press it very close to where they want that information to be passed. So it's not something that's radiating a beacon around you of all of your account information. It's something that's very tuned to a specific interchange between a reader device and a card.

Even if somebody would introduce a reader device that's more powerful with a greater read range,
the amount of range that is increased by that
significantly deteriorates the information that is
transferred between the card and the reader.

And then the more important aspect of it is
whatever that information is that's being read off the
tag, what can someone do with that information? And
that's where we have to look at in terms of the card
number and the value that's on that card is a unique
number for one transaction only.

If somebody were able to read that information
and then try to replay it or reuse it again in other
payment transaction, the system would reject it.
There's no personal data on the card. Your address and
your Social Security number and all of that that some
people speculated is not part of the payment platform.

And there really are some very sound
principles behind security and privacy issues around
contactless payment, and I'm sure the people that are
going to be following today's panel will cover those in
more detail.

So in the limited time I had, I wanted to kind
of give you that framework of the discussion for today
and highlight for you that there's many, many more
resources for you.

If you're a reader and want to understand a
lot about what's happening in contactless payment, I encourage you to go to the Smart Card Alliance website, www.smartcardalliance.org, and there's a wealth of information that is available to understand how this technology works and how it applies in the industry.

And I'm going to hold my questions because I want to give Dan his equal time as well. At the end, we can take questions. Thank you.

MR. LITTMAN: I'm Dan Littman. I'm with the Federal Reserve Bank of Cleveland, and I do a lot of research on the payments system; although most of my research has been on the traditional side of the payment system as opposed to cards. And I'm going to talk a little bit about that in the context of cards.

So I wanted to provide some context of where cards and contactless cards sit in terms of the broader payment system, particularly retail payments, and why we care at the central bank about something that we're not involved in directly as an operator.

So contactless cards are one of many innovations and actually traditional instruments that are out there in the payment system. It's kind of like the Where's Waldo, who actually I had to insert in the picture because he wasn't there.

And, you know, we're going through a period...
now in the world, especially in the developed world, and the United States being part of that, where there's more payments innovation than there ever has been before. And, of course, that's all caused by the information revolution and computer technology. It's not caused by anything that's unique to the payment system. And contactless cards are just one of those innovations and probably not the most important of those innovations in terms of the current time.

Probably the most important innovation in terms of size is the area that I've got in that yellow circle. So Check 21, image replacement documents which are part of Check 21, the image exchange, which is related, and then all the different check to ACH conversion technologies or work types that the National Automated Clearing House Association has introduced in the last five or six years, that's the most significant innovation in the payment system because it's having the greatest impact on the number of transactions. And, of course, there are a lot of innovations in the Internet space. So contactless is just one of those.

Randy mentioned top of wallet, the goal of all these payment innovations, particularly the ones that are carried around people's pockets or purses is to get to top of wallet. And contactless is very far from
being top of wallet. It's not even top of wallet
probably in Hong Kong or Tokyo or London. Maybe for
some people, but certainly not for the masses.

And the reason for that -- the most important
reason for that in the United States is bank notes and
coin, which is the elephant in the room that, you know,
card companies -- we all acknowledge. We all know it's
out there, and it dominates retail payments in the U.S.,
although nobody really knows how many transactions there
are. I kind of made up a number that -- Global Concepts
made up a number, and I used their number.

So probably we have somewhere in the area of
200 billion transactions in the U.S. that are in the
retail space, and roughly half of those are cash still.
But nobody really knows how many cash transactions there
are. It could be 80 billion, it could 120 billion;
we're not quite sure. The rest of them we have a pretty
good idea.

And, again, contactless is a relatively small
player in there. That doesn't make it unimportant, but
it's much smaller than check, which is declining. It's
much smaller than ordinary debit transactions, which
have surpassed credit cards and continue to grow much
more rapidly than credit cards, and it's smaller than
ACH and so forth, which are more entrenched and more
traditional payment vehicles.

Payment instruments all go through a life cycle. They're born. A lot of them in any innovation space in any industrial segment, they don't survive infancy basically, but some of them go on to adolescence and become mature technologies.

When you look at the payments based today in the U.S. and actually in most developed countries, the mature vehicles are cash, checks, automated clearing house or whatever name they might go by. And over their infancy, you have a lot of internet-type vehicles or instruments, some of which won't survive, or if they do survive, will have a new name by the time they get to adolescence.

And I would put contactless cards somewhere in between infancy and adolescence. Certainly, in the transit space, they're probably entrenched, but in other places like going beyond fast food and other segments where they are important, they're still in their infancy.

The payment system is something that evolves. It's not something that has revolution that occurs in it. And so contactless or any of these other innovations, they're all based on all the previous innovations that occurred before them. And, you know,
contactless is something that grew out of cards and
which grew out of other payment technologies, and so
it's not something that just is in its own silo. It
sits on top of all the other payment technologies that
exist.

And, you know, even contactless is relatively
new, certainly in the context of those other payment
instruments that I showed, it really derived some
strength from being old in terms of where the technology
came from.

So some of it came from the development of
Identification Friend or Foe technology for aircraft
during World War II. Obviously, some of it came from
the origin of credit cards or travel entertainment cards
in the early '50s and other technologies. So it gets a
lot of its strength from being built upon a
technological basis over 50 years old, even though it's
something relatively new in people's pockets.

Contactless in a niche product. So it's
not -- you know, it only dominates -- actually, it
doesn't dominate any market really, but it's only
important in a few markets today, and those are mass
transit, fast food, drug stores, and some of the other
areas that Randy mentioned.

And, of course, it aspires to be dominant or
at least present in every market. And over the next 10 years, it will. In the next 10 or 15 years, it may do through a mobile form factor as opposed through FOBs or the other form factors that are available.

And, as I said, contactless builds on what existed before. Randy has talked about this a little bit. It involves most fundamentally the few centimeters between the card and the point of sale device. And after that, it's riding on the infrastructure of the card system.

So the risks are out there in the card system, whether you're talking about TJ Maxx losing information or getting information compromised or Hannaford Brothers Supermarkets, those things are shared between the card system and contactless. And whether there were any contactless -- I assume there were no contactless transactions in those two cases and most other cases because most of the card transactions are traditional.

Why does the Fed care about this? Sometimes I wonder too. So, you know, the Fed, don't we run the declining part of the payment system? We do. But it's still a huge part of the payment system. Still there's about 30 percent -- we process about 30 percent of the checks, and checks still represent 30 percent of all the payments that are not made in cash, but declining.
So why are we concerned? And I'm speaking for Dan, not the Federal Reserve. We're concerned because as a central bank, we're interested in the efficiency of the payment system. We're interested in access to the payment system, and we're interested in the risk of the payment system. So in terms of efficiency, all payment systems create friction. You know, you have to keep the economy lubricated in some fashion, and the payment system is one of the things that does that.

And there have been estimates sort of made up that suggest that the full cost of the payment system in the U.S. and actually in other developed countries is somewhere between a half a percent and a percent of GDP. And, you know, that's about 140 billion dollars. It's a lot of money. It's one and-a-half times U.S. spending on liquor. So, you know, you can get some sense of its size. One-third of U.S. spending on purchase of new cars, at least before the current economic -- whatever situation we're in -- downturn.

So it's a very large expense, and anything we can do to make it lower allows people to use the extra money to buy more liquor or pay baseball players more money.

So contactless is something that creates more efficiency in the payment system, and Randy has talked
about that a little bit, in terms of the speed of buying
hamburgers at McDonalds or whatever or buying gasoline.

In terms of access, you know, from one
perspective, the contactless doesn't improve access
because it's really just a substitution between a
traditional debit transaction and a contactless debit
transaction, especially if you're thinking about beyond
mass transit.

But it does create some opportunities for more
access by people who are unbanked or underbanked. And
probably we're seeing this more in the countries like in
South Korea or in Hong Kong or in Singapore where people
are using cards like Oyster or Octopus to make
transactions outside the transit space with cards that
were intended for the transit space.

And we're starting to see some innovation
using contactless in mobile phones in places like Kenya
and West Africa where contactless is being used to bring
into the payment system that wouldn't otherwise have a
bank branch or any other method of being in the formal
payment system. So it has some opportunities to do
that.

How much we do it in the United States as
opposed to in South Africa -- it's going to have more
impact in South Africa or Kenya than it is on the U.S.,
but it could bring some people into the formal payment system that are not today there.

In the Fed, we're interested in risk. We're interested in systemic risk, which probably is another term for a crisis starts one place and then it moves through the payment system and the financial markets to the wider economy. So that's sort of what occurred with Bear Stearns earlier this year.

Does contactless fit into this? No. No retail-type transaction vehicle has characteristics of systemic risk in most developed countries. So we're not worried about contactless in terms of systemic risk. We're interested in bank risk along with all the other bank and financial institution regulators.

Does contactless pose a threat that would cause a financial institution to fail? Whether spread elsewhere, that doesn't seem to be the case. So, you know, what happened to IndyMac, which is not an institution that the Federal Reserve regulates, had nothing to do with payments and had no consequence on retail payments.

But, you know, we are interested in consumer risk, and along with the FTC, we're one of the regulators of consumers through -- or consumer rules through the Regulation E. And there we are here or I'm
here to try to learn more about what other people think
about risks in this area.

So these were the areas -- the topics I
covered, and I think we have time for questions or
hopefully we have a little time questions.

MS. HARRINGTON-MCBRIDE: I think we have about
a minute and-a-half for questions. So if you can talk
fast, we'll answer quickly too.

Does anybody have any questions in the
audience? It's because we didn't provide coffee, isn't
it? Yes, Eileen.

MS. HARRINGTON: I was interested in your
comment about security. Early on, you said most
important -- that the most important innovation
happening in the payment space right now is Check 21 ACH
demand draft, that whole area of remote access checks.
Do you think that, for consumers, contactless payment is
more secure -- is safer for them than those remote check
sorts of payment options?

MR. LITTMAN: I guess I wouldn't weigh them on
a scale like that. The one thing I would say is that
people are not aware of the risk aspects of the dominant
payment vehicles. Just like on anything, we focus on
the new types of vehicles, whether it's Obo-Pay or
contactless payments or PayPal. We focus on those
because they're new and novel, but we don't focus on all
the risks -- characteristics of check clearing.

You know, checks -- before Check 21, the
average check was handled, you know, 15 times between
the time you paid it at a retailer and it arrived back
at your bank and it was put into an envelope and mailed
to you. The opportunities for fraud in check -- and in
addition, in those days, people sometimes had their
Social Security numbers on their checks and certainly
their phone numbers -- are much greater than people
realize.

Now, how that balances with cards, I guess I
wouldn't be willing to say, except that all these
electronic vehicles are not handled many times and have
less opportunities for fraud to occur than you have with
check or, obviously, with cash, as Randy said.

MS. HARRINGTON-MCBRIDE: Jean, one quick
question from you, and then I think we'll cut it off and
move on to our consumer panel.

MS. FOX: Dan, you mentioned that contactless
cards can extend access to unbanked consumers. Does
that assure us that the Federal Reserve will extend the
Electronic Fund Transfer Act protections from payroll
cards to general use store value cards?

MR. LITTMAN: You know, I know that they have
changed the rules so that payroll cards are covered, and I know they have thought about the traditional or the prepaid cards. But as far as I know, there isn't any work going forward at the board or something that the Board of Governors does to do something about what is now really a state regime for prepaid cards -- for store prepaid cards.

MS. HARRINGTON-MCBRIDE: With that, I'm sorry that we don't have a little bit more time for questions, but as Chuck mentioned, we're going to have informal opportunities for gathering and talking. And I hope that if you do have questions for the panelists, you'll stick around and chat with them at the break and at lunch.

And with that, we'll conclude this panel. Thank you very much for your attention, and we will look forward to hearing from Chuck Harwood and his panelists on consumers understanding and acceptance of this technology. Thank you.

(Recess taken.)
MR. HARWOOD: So this is the next panel in our program today, and it's entitled, Consumer Understanding and Acceptance of Contactless Payment Technology. And as with the previous panel, our plan is to have each individual provide their -- each panel provide their presentation, and then we'll take questions at the end of the presentations. I may intervene with one or two questions, but for the most part, we'll wait until the end to take all questions.

In terms of the order we're going to go in, we're going to go in the order they're actually seated at the table. That was good planning. And we're going to start with Jodi Golinsky and then move on down the panel.

And Jodi is with MasterCard. She is the Vice President and Regulatory and Public Policy Counsel for MasterCard. She joined it in May 2003. You can find more details about Jodi's impressive resume in the bios section of the materials in your folder, as you can also find out about our other impressive panelists by looking in the bios section. So with that, let Jodi lead the way.

MS. GOLINSKY: I also want to thank Julie
Mayer and everyone from the FTC for organizing this conference. I applaud you for bringing us all together to talk about this issue, which is important to consumers and, of course, is important to MasterCard as well.

I didn't realize that I was going to have to follow Dan with all those very funny cartoons and graphics, which leaves me feeling a little insecure, but I'll do my best. I do have a video, so maybe that will help keep me at a level playing field.

What I'm going to try to touch on today are just three major things and give brief comments on all of them.

And first what I'm going to talk about is just what MasterCard's contactless technology is, and what consumers know about it and sort of the acceptance of that. And our version of contactless technology is called PayPass. So I'm going to give you some background on that, and also what we believe, through our own benchmark studies, is the acceptance that consumers have for that technology.

And I am also going to then touch on the two issues that seems that most consumers bring up or consumer groups, which is the points about security and privacy, just to reiterate some of the points that were
already made on the last panel about what the security
features are on these cards and sort of how they work.

I really like the image that Dan gave you
about the evolutionary piece of this. I think there are
a lot of misconceptions about contactless and what it is
and what it is not. So, hopefully, through my
discussion about what MasterCard has done with PayPass,
you will see that there are a lot of things that PayPass
is and there are a lot things that PayPass is not.

And one quick thing that I'm just going to
mention, just since this is an open forum, and I don't
usually do this in this context, but just to give you a
better sense about what MasterCard is, MasterCard is a
brand. And what we do as a company is we license our
mark and our brand to customers who are financial
institutions who then use our brand to issue cards or
sign up merchants to take our cards.

And I just mention that because it's an
important thing to note that we work very closely on the
PayPass product and technology, but we are not the ones
who actually offer that technology out to consumers --
that's done through our customers who are issuers who
will make that technology available to you.

And I mention that only because certain
questions you might have about what's done or what
communications are made, MasterCard really works hard to educate consumers about PayPass, but so do our issuers who are the ones who are actually issuing you those cards that have that functionality.

So before I start, I want to just get you a sense of PayPass and its footprint, and I'm going to do that through a video that I hope is ready to play.

(The video was played.)

MS. GOLINSKY: So that was just to give you a sense of sort of how PayPass has evolved in terms of numbers. And, actually, our quarterly numbers are coming out this Friday. So we don't have new numbers for you, but as of the first quarter of 2008, we had 28 million cards or devices issued globally that were PayPass enabled.

And an important point to make, and I think in one of the prior presentations there was a mention about contactless being for debit. Actually, the PayPass functionality runs the spectrum of all of our products. So it's not just debit. It's credit. It's prepaid. Any MasterCard product can be PayPass enabled. So it's for the whole gamut of our products.

There are 24 countries right now where deployments or consumer trials are taking place, and we now have acceptance outreach of 109,000 merchant
So you can see that this is something that is taking off, and I think that's sort of the theme of today. This is a technology that's really on the move, and it's starting to rise. And what do consumers think about it?

One of the things that I think is important to just mention is what PayPass or what our technology is not. And this is based on a lot of the things that I read, comments that were posted in some papers that you read about this.

This technology, at least with respect to payment cards, is not a tracking device. It's not used for inventory control. There's nothing about this transaction that would make it different in terms of tracking you or your personal use of a card any differently than if you used your credit card.

So while there are some fears, I think, about it being some kind of an internal GPS device following you wherever you go, it's no different than using your credit card or debit card or prepaid card in any way than you normally would.

What does MasterCard do to give consumers a little bit more information about these cards? And I was talking to Jennifer earlier today about her studies,
and she did some studies a year ago and I know she's
going to start doing some additional ones. I think what
we're seeing as we see a greater take-up of this
technology and interest in this kind of payment is that
we are reaching out more to consumers, us and our
issuers, to make that they understand what it is.

MasterCard has a whole website devoted to
PayPass. If you go to MasterCard.com and click in
PayPass, it will take you to information about the
security features on a PayPass card. It will take you
to information about what are frequently asked
questions, what is this technology, what does it do, how
does it work. So we're really getting out there more
and educating consumers about this, and they like it.
So one of the things I would say is you should certainly
take a look at our website if you're looking for
information.

And we work with the issuers who are going to
do programs that are PayPass enabled to provide them
with communications that they can provide to their
customers to explain this technology better.

Another important key piece about this is the
zero liability piece. MasterCard offers zero liability
on all its payment cards, PayPass enabled or otherwise.
So that is a huge consumer security feature -- it's not
a security feature. It's a feature that gives you piece
of mind that if for some reason there is anything
fraudulent going on with your card or unauthorized
purchases, you have the luxury of zero liability on all
your PayPass enabled cards.

What MasterCard has also done is some studying
and some benchmarking, and I can't actually provide the
entire study because it's proprietary, but I will tell
you some of the results, and we're obviously undergoing
additional study.

But in 2007, we did a benchmark study on
consumer satisfaction to try to learn how consumers were
reacting to PayPass in the early years of the product
introduction. And our study consisted of eight issuers
and telephone interviews, 15 minutes, and 400 interviews
were conducted for each issuer asking a variety of
questions about PayPass cards. And these were
individuals who actually had PayPass cards in their
possession.

And without going through all the results, one
of the key results is that 90 percent of the respondents
said that they were very satisfied or somewhat satisfied
with the card. And 87 percent said that PayPass met or
exceeded their expectations.

So what we're seeing is that consumers really
like this. They like the efficiency. They like the speed. They like the convenience, and it's targeted to places where speed and convenience are important. And, of course, MasterCard is going to continue to test and monitor, as well as our issuers in doing that.

I'm mindful of my time, so I'm going to go very quickly through security and privacy, but they are important pieces. And if there are questions, you should please ask me about them at the end.

Our cards and devices are processed through the same financial payments network that processes all of our magstripe, and Dan made that point as well. So to the extent that there are security concerns about PayPass enabled cards, there are security concerns that would apply to anything, because what we're talking about is transactions that run across our rails. And all of the protections that we have for any of our transactions apply equally to our PayPass enabled cards.

Now, of course, the PayPass enabled card is different because it has this chip technology and you have the radio frequency. So MasterCard has a number of security features in place to try to address that. And one of the things that I can mention is that we now mandate that the cardholder name cannot embedded into a chip on a PayPass enabled card.
In a lot of the research papers I read and comments posted, there was concern about the privacy piece that your name somehow is getting out there. Somebody could, if they were able to get a reader, could read personal information about you. That's not the case because MasterCard now mandates that the cardholder name cannot be embedded in the chip.

Also, the way these transactions are valued -- and I'm not a technologist, but I do understand this in my layman terms, and I'll explain it to you in those layman terms is we have something called Dynamic Card Authentication for these transactions. It's called Dynamic CDC3. And so what happens whenever you do swipe or touch your PayPass to the reader is that a value is generated for each transaction, and that value is unique and cannot be replicated. There's a key that's part of the chip, as well as a three-digit number that is an unknown, unpredictable number that goes for every transaction. So the chance of replay fraud is extremely low, if not impossible, because each transaction has a unique value.

And MasterCard used to have that as a best practice, but we have now mandated that all PayPass enabled cards have Dynamic CVC3 in them.

I was going to say some more, but I know that
my time is up. So I will pass to Jennifer, and I'm happy to take questions at the end.

MR. HARWOOD: Jodi, just one quick question. You talked about replay fraud. Can you explain what that means?

MS. GOLINSKY: Sure. The replay fraud, the concern is that somebody -- at the same time that you are doing your radio frequency, you're tapping your card, that somebody else is reading into that and reading the same values, and then would take that same information and then try to do another transaction at that same time or in another location.

Each transaction now has this unique code, and it's combined with the CVC code, this 3-digit number and something else called an application transaction counter. So that even if somebody were to read that from some other distance, they're not going to be able to replay that transaction.

MR. HARWOOD: Thank you for clarification.

Our next speaker is Jennifer King. Jennifer is with the Samuelson Law, Technology and Public Policy Clinic at UC Berkeley School of Law, and, again, you'll find Jennifer's more complete bio in our materials.

Jennifer is going to talk about a study she's currently engaged in that is directly on point with the
grander interest in consumer acceptance and understanding with regard to contactless payment technology.

And I think you have a Power Point?

MS. KING: I do. Thanks. Thanks to the FTC for having me, and thank you especially for not making me travel to D.C. for once and staying on the west coast, much appreciated.

So as Charles mentioned, this is a preliminary study that I started last fall, and it is available on the website. And if you have specific questions about it, please ask me afterwards and I'll be happy to answer them for you.

So I am a -- I call myself a social technologist. My educational background is in information science, so that I work at the equivalent at UC Berkeley to the clinic here at UW. So I work primarily with lawyers, but I, myself, am not a lawyer.

So this study we started, again, last fall. Again, this is very preliminary, and we'll be finishing it this fall with a much larger number of subjects. And so the premise for doing it was that we feel that RFID is a somewhat new, relatively at least in terms of what consumers see, and a socially disruptive technology with the potential for changing how people really interact.
with their every-day environment.

And so we wanted to find out how people actually think about RFID, if they actually understand how it even works, and how they actually expect it to work, because we think that there are potential security and privacy implications to how people either understand or misunderstand how the technology actually functions.

And so we looked at objects in two primary domains. We looked at consumer commercial uses of RFID that was focused on credit cards, and then we looked at what I call the public domain, and that's the ePassport and public transit cards. And for Randy's benefit, I'll mention that we are looking at contactless smart card technology here and not the type of RFID that you're thinking about in the supply chain where you're seeing tags on boxes. These are, obviously, far more sophisticated than kind of basic RFID.

And so we investigated something we call mental models, which I'll explain more in a minute. And we are looking at how people understood radio frequency in general and how they understood RFID specifically. And so these findings are, again, preliminary because we started with a very small sample, nine subjects. We put it out there at this point because we wanted to get feedback on how we designed it to see what we wanted to
do for the next round of testing.

And so we focused on trying to find three

novice users; people who had no concept of what RFID
was, three intermediates; people who had heard of the
concept but couldn't necessarily articulate what it was
and how it worked, and three experts; people who really
did actually understand what it is and how it worked,
and so, again, with the transit cards, credit cards and
the ePassport.

And my focus was really to try to study real
world objects that people already had in their hands
rather than, you know, prototypes or something that
wasn't in wide use at this point.

And so just very briefly, in exploring mental
models, what you're trying to do is look at how experts
design the system and how your end users understand how
that system works. And you're trying to reconcile the
two things so that you understand where the flaws are as
an expert in your models so that you can build something
that your users actually can comprehend and understand
and use in the real world.

And so the way we tried to test this is that
we tried to get users' mental models of how RF
technology worked in general, and specifically how they
understand -- how they understood how the RFID enabled
object that we were testing worked specifically.

And so what we started off by doing is giving our subjects a very short survey, which is in the appendix of my study, just to get a baseline measure of their attitudes toward the technology and how they understood it. And we included questions about other RF enabled objects such as key FOBs for opening car doors or badges for getting into buildings, trying to get a triangulation if they understood how these things worked or, you know, what their best guess was.

And after we took the survey, we basically conducted a one-hour interview. We talked through the survey results with people and we asked them more specific questions about whatever object it was that we had recruited them for.

And in that hour, we generally gave the users documentation that we got from either -- in the case of credit cards, from either the credit card websites, for example, or other marketing materials we found with the e-Passport. We included the brochure that actually was mailed with the e-Passport when you receive it, to walk through those official documents to see if they gave people a better understanding, again, of what technology was included in this object and how it worked.

So we looked at -- we talked to a handful of
UC Berkeley graduate students, some staff members, as well as some members of the public. About half of them were technical and half were not.

And what I expect to find when we do our next round, that most of the people we talk to probably will not be technical. Even though we are in the Bay Area, so there's generally a higher technical knowledge, I think, in the public, we'll probably find a lot less specialized expertise than we did with this sample.

So generally early 20s to early 30s, most had heard of the term RFID, even if they didn't know what it stood for. Half of them had no understanding of how it worked. They could not explain what it really was and what it did. And so we looked at some very personal usage scenarios.

So with transit passes, we found that the majority of the people who use these were very comfortable with the idea of what a transit pass was and how it worked.

We mentioned in our survey keyless entry into your home as an example of something you might use in the future, and most people were kind of very mixed on that idea. They liked the idea of actually having a physical key in their hand to open their front door.

Credit cards we actually found that over half
the people we talked to were very uncomfortable, and I think that's largely because, at that point, most of the people we talked to who had the credit cards either hadn't really used them yet or they were so new, they just didn't have any real experience with them in the world. And so for them, at that point, it was still a big unknown quantity.

And the e-Passport, the majority of them were definitely uncomfortable or uncertain with the idea that it had RF technology in it. They didn't see why, for example. And so I may go through these just point by point.

With transit cards, what we looked at in the Bay Area is the Bay Area Rapid Transit System. They have been piloting a contactless transit card now for about -- I think about two years.

And so the structure of that interaction, the idea that you can just walk through the turnstile, have it read the card, they get some kind of visual feedback or a beep that it's actually been read, the fact they don't have to wait in line, that all really made sense to people with regards to transit. It had really obvious benefits and efficiencies for people who didn't have to wait in line. They didn't have to deal with paper tickets. And just like the D.C. Metro where it
uses these paper tickets, generally that if you get them wet, they just fall apart and they stop working. So the idea of a plastic card really made sense to people.

And they also saw that there was very little personal risk to them because they didn't think that the BART card could potentially store any personal information about them at all. And they also didn't see potentially any threat that anybody could get access to their transit history and find any value in that. So they thought really in terms of their personal risk, it was very low.

So with the contactless credit cards, the people we talked to really did say they saw very little benefit in terms of the efficiency gained because they didn't see why it was necessarily faster for them versus just swiping a card today as you do at most pay terminals.

Many of them were very concerned about the security of the entire system. Identity theft was mentioned quite often in our talks. And financial data was seen as something far more personal to them. They had much more of a personal impact if something was compromised. And, interestingly, most people actually said they wanted what they called the security of signing for a purchase.
A few people had already experienced the new change, which I think it's either under 15 or under $10 or maybe it's under $25 transactions where you no longer necessarily have to sign. Most of them were very concerned about the fact that they didn't have to sign anymore. It didn't cognitively make sense to them, even though I don't think those signatures in general really mean anything. My colleagues in the credit card industry can probably clarify that, but I think it's kind of a false sense of security is my understanding. But for our users, it really did mean something.

And they're more comfortable with just the idea of something like a transit card where you're using it for a single purpose rather than this kind of general use card which you could use everywhere at this point. They just really didn't conceptually understand why they would want to do that.

And then, finally, the Passport. This was the one where, in particular, people really didn't feel like they had any benefits. Obviously, this is not a payment system, so not as relevant for our discussion today. But just, in general, people didn't see that they had any personal benefit from the fact that RF technology was included in the Passport. They really thought it was only going to benefit the government, and
they especially didn't see why it needed to be remotely readable. It just didn't make sense to them.

And their concerns about security were highest on this because they knew that personal identifiable information was included on the Passport. And so they said things like, the stakes really seemed higher.

And for a couple of our respondents, they were naturalized citizens, and they felt like the Passport was the only thing that really showed that they were American. And so in that sense, they just thought it was a lot more of an important thing that the security of the Passport remained high. And they really articulate a lack of faith that the government, in doing so, is really looking out after their best interests.

And the Passport was the one thing in particular that when people actually looked through the official documentation, they were generally left more confused than they were before they even read it. They felt like they just didn't have any sense, after they read the pamphlet that came with the Passport, about what it was, why they did this, what the risks could be -- potentially be. They ended up generally, like I said, more confused than when they started.

And so the commonalities that we found across all these three objects was this notion of convenience
and efficiency, which you've already heard several times today. Certainly, that's, I think, a benefit the industry is talking about, and it is one that consumers are seeing as well.

One of the other things I found is that -- I call this, Where is the Beep? There was a universal expectation that whenever a card was read, that there would be some type of audio or visual feedback. And that's a really important point because RFID readers do not have to give you audio or visual feedback. It is generally our expectation that they will, but they don't.

And that's especially true if I am, perhaps, using a RF reader to illicitly read something. I can, obviously, turn the beep off, for example, on many of the readers I own. So I don't have to give you the signal if I'm reading something. So it's an important thing to realize that people expect it, but it is not necessarily default behavior of the technology unless you implement it that way.

And then the context is really important, which I think is an important take-away for today, which is whether or not the use that you're trying to put forward really aligns with how people expect it to work. And, you know, we were left with the question after
doing this is if we thought the issuers had more
benefits with using this than the actual users.

Just very briefly, just notice and consent
issues. None of the people that we talked to were
really made aware from their issuers that the credit
cards they received contained an RFID chip, Passports,
what have you. The only exception, that was the BART
card because you to actively solicit to get the BART
card. And those who were aware of it were generally
made aware by the media or by their friends, but not
necessarily from the issuer themselves.

And although this was a year ago, so the
educational materials will obviously probably change by
the time you look at them again, most people -- at least
a year ago, nobody was really explicitly talking about
the fact that these cards contained RFID. And so most
people didn't have any understanding of what it was or
what the risks were after actually looking at the
official documentation.

I'll go ahead and stop it there.

MR. HARWOOD: Jennifer, I have one quick
question for you, and it's stated in your summary of
your written materials. You talk about the fact that
depending on the type of form factor that's being used,
that changes the level of consumer understanding. Did I
read that correctly? For example, it appears that in a cell phone, which consumers are already commonly used to using, that's more confusing for them potentially than it appears than if something is a kind of new form factor they're not familiar with in terms of their understanding of how the system works or what their concerns should be about --

MS. KING: Possibly, because I don't have access to industry research, and I haven't done any research on phones myself. I would imagine it's -- I think of it as like camera phones, for example. You know, 15 years ago if you told us that not only would you have mobile phones, you'd have cameras in your mobile phones, most of us would have been perplexed as to why you'd ever want a camera in a mobile phone.

But today, it's -- well, A, it's difficult to even get a phone now without a camera in it. This is actually something we studied at Berkeley, where we found that people really adapted to the inclusion of the camera, and they use it in ways that -- when you thought about photography 15 years ago, you would have never thought that you'd take a little tiny 640 X480 picture of something and it would be of any use. But, instead, we find that there's actually really good uses for using cameras in phones.
I would expect integrating payment into phones is going to be very similar. I mean, you'll have people who will just -- there's a good study done by Nokia actually where they were testing out Nokia NFC phones. And they had a poster they put up with either a 2D bar code or an RFID tag on it, and they basically walked around, I think, Helsinki asking people to figure out what to do with the phone and the poster.

And what they found is that people who were using the 2D bar code, it really made sense. This is actually something we confirmed as well, is that people understood the optical scan portion of the technology. So that the 2D bar codes, the people went, oh, well, I think I use the phone. I take a picture of the bar code, and they figured out how to interact with it.

With the RFID, they just kind of looked at the phone and pointed it and took pictures, and most people didn't realize they could just tap it on the tag and have it work.

So it's a question of can we teach this to people or, you know, does it -- is it something that's so unusual it won't make sense in the context of how they operate.

MR. HARWOOD: Thank you, Jennifer.

So our next speaker is Jean Ann Fox. Jean Ann
is the Director of Financial Services for the Consumer Federation of America, an NGO or a non-profit association with more than 300 consumer groups around the United States.

MS. FOX: Thank you. Good morning. It's good to be here with you in Seattle.

If you had to have a slide for me, which I didn't provide, it would be Dan's last slide with a, you know, befuddled looking person and all of the math in the background. I'm not your technology one.

But I do want to talk to you a bit about mobile payment devices from a consumer financial and consumer protection standpoint so that those issues get included in our conversation today.

And a lot of my work involves working on financial service products that are used by cash-strapped families, low-income consumers, folks who may be outside the mainstream of banking.

And I'd like for you to just bear in mind that some of the selling points for the contactless payments and the convenience of just tapping a card or tapping your phone to make a payment is -- this is likely to encourage consumers who have trouble making ends meet to spend more money than they would have if they pulled cash out of their pocket. That's one of the selling
points; that it increases the size of an individual purchase, that you're not constrained by how much you have on you.

And so one of the things to keep in mind is does this help consumers manage their scarce resources or does it just make it easier for you to go broke faster.

Another question also comes to mind is who's going to pay for all of this? The investment in deploying all the point of sale readers and having all of the players involved -- one of Randy's slides, there could be nine different players involved in a contactless payment arrangement. All of that costs money. And as our Federal Reserve points out, the payment system cost is not an inconsiderable amount of money. So where does the buck stop on that? And of course my view is the consumer always ends up paying.

So in this situation there are two ways that this is going to get paid for, either larger transactions, more frequent transactions and fees that get assessed at every step of the way or in the currency of consumer personal information.

If you're paying with cash, there's just not a trail of where you spent your money and how much you spent. Once you get people into using plastic or their
cell phone or whatever the next whiz-bang application is
going to be for contactless payment, now you create a
record and a paper trail -- not a paper, an electronic
trail of where money was spent, how much was spent.

And so as one of the slides pointed out,
targeted marketing becomes in loyalty programs, becomes
a benefit to merchants. Well, that can be considered a
cost to the customer as well.

A lot of attention is being applied to the
privacy and security issues that go with contactless
payment, and just a few points from our point of view
about that. I understand that a lot of the contactless
payment now is running on the regular systems we have
for credit and debit, but this is going to move to cell
phones.

And the information that's stored on your cell
phone with your passwords and a lot of personal
information -- people use their PDAs almost as their
computer in their pocket. All of that information is
going to be available, and the protections that go with
the security aspects of contactless payment are going to
be extremely important. This adds location information.
Not only how much did she spend and where did she spend
it, where is she at the time that that transaction is
taking place?
This can be used for profiling. It can be used for proximity marketing. There was the movie where the guy walks through the store, and the ads come up and say, Jennifer, I see you have on a --

MS. KING: Minority Report.

MS. FOX: Oh, yeah. And, you know, is that going to happen? We'll see.

Another aspect of privacy that we've all taken for granted for the decades ago when the OECD annunciated them is the Fair Information Practices that ought to go with consumer information.

But, you know, where did consumer choice come in here? Did all of the millions of cards that have been circulated with the speaker doohickey on it, did consumers ask for that? Did they have a choice? Were they able to say, I want a credit card, but I don't want a chip on it? What kind of notice or consent was involved? And can you have a card that allows you to tap it but not be tracked on your purchases? So there are questions.

And in looking at the commercials that we saw where the elephant goes to the store and uses the sick guy's card to buy cough syrup for him.

MS. GOLINSKY: It's his own card, actually.

MS. FOX: Was that the elephant's card or was
that sick guy's card?

       MS. GOLINSKY: He's going to get his sick
friend some medicine, but it was his card.

       MS. FOX: Inquiring minds want to know.

One of the issues I would bring up with you --
because you're going to hear a lot about security and
privacy as the day goes on, but I want to focus on the
payment card protections that I think are responsible
for the consumer confidence, and it's okay to wave your
credit card around or the debit card that draws money
out of your checking account because we have a framework
of federal consumer protections that make consumers
comfortable in handing, you know, some clerk their card
or using it in a contactless setting.

       So for credit cards, you're protected by the
Truth in Lending Act and Fair Credit Billing Act. You
know that you have, at most, a $50 liability limit for
unauthorized use. You know that there are dispute
rights. You know you can charge back a transaction. If
the thing didn't come that you paid for, then you can
dispute the bill. You aren't out any money while it's
been investigated. Consumers are comfortable using
credit cards because the Federal Consumer Protection Law
provides some real protections.

       There are protections that go with using a
debit card that pulls money out of an account in your name at the bank. They're not as good as the protections for credit cards, but there are rules there. But as we've been told this morning, you can use contactless payment with stored value cards. Those are gift cards, payroll cards, general spend debit cards, the kind of cards that are being sold to unbanked consumers to load their paycheck on it at Wal-Mart or at check cashing outlets or other non-bank financial service providers. And these cards can hold considerable family resources.

We do not have a Federal Stored Value Consumer Protection Act. And depending on how the cards are set up, consumers may not be protected by a federal provided liability limit. There are no clear dispute procedures or time limits. There are no charge back rights. There's no right of free credit if money is taken off your card that you didn't authorize because the machine hiccupped and processed it twice. You can't call up and say, put the money back while you investigate it. You're out the money.

So the deployment of contactless payment and the new forms of it that are going to come shine a bright spotlight on the fact that we need to have uniformed, consistent, high-level protections for all
forms of payment so that consumers don't have to scratch their head and say, is this card that's plastic and has a MasterCard or Visa logo on it, you know, am I covered by Truth in Lending? Am I covered by Electronic Funds Transfer Act? Am I covered by the Fed's rules on payroll cards? Am I not covered by anything? Should I feel safe in using this card?

And I hope that the companies that want consumer adoption of contactless payment will be at the head of the line in advocating for high-level, uniform, clearly-understandable payment card protections.

Just think about if we get to the point where you can pay with your mobile phone. If the payment is being processed as a credit card, you're protected by Truth in Lending and the Fair Credit Billing Act. If it's being processed as a debit transaction pulling money out of your checking account, you're protected by EFDA. If the bill -- if the payment goes to your mobile phone bill, you're not protected by anything at the federal level.

And I think that the fast pickup and the comfort people feel with these cards is a direct result of federal consumer protections, and we must upgrade them for all forms of consumer payment so that the new forms of payment are safe for consumers, there are clear
protections against an unauthorized use, there's a
dispute process, you can charge back an unsatisfactory
transaction.

I mean, think about it. Today, the most
affluent consumers who have credit cards have
charge-back rights. Poor people, who can't afford to
waste a penny, who use store value cards, don't. It
makes no sense.

MR. HARWOOD: Jean --

MS. FOX: I'm through. Thank you very much.

MR. HARWOOD: You have another ten seconds or
so, but that's fine.

MS. FOX: Well, then let me say one more --

MR. HARWOOD: You can have ten seconds.

MS. FOX: The card companies are happy to
advertise their zero liability limit, but if you look at
the footnotes with the asterisks, those are much more
limited than you might believe.

So Visa's zero liability limit applies if you
use the Visa system, not if you take yourself down to
the ATM, right?

And MasterCard's zero liability doesn't apply
if you've had more than two unauthorized transactions in
a year. So somebody, you know, has skimmed your numbers
and has been putting charges on your card or taking
money off your card. If that's happen more than twice, does the liability limit apply?

So although we always encourage industry to do the right thing and to have good standards and best practices, nothing beats enforceable federal law. Thank you.

MR. HARWOOD: Thank you. And I actually have a question. Let me just ask it -- actually ask, Jodi, if you would like to respond to the elephant or something else?

MS. GOLINSKY: No, I said my peace on the elephant.

MR. HARWOOD: Let me just ask you, Jean, real quickly, when we talked during the early days of the Internet, we used to talk about the problem of old wine in new bottles. We used to see old problems appearing in a new media environment. Is that essentially what we're looking at here or do you see this as being -- because you're talking about the same sorts of protection issues that you would -- that you see already. I mean, is it something different when you're talking about debit cards or the same thing.

MS. FOX: No, this is different. And take the example of the Scandinavian countries, where they're now making payday loans using somebody else's cell phone.
They're called a short message service loans. So the young folks are out partying on a Friday night and run short of money. They text their request for a cash infusion, which gets loaded on their debit card. They pay 800 percent interest, and you've got to pay it all back in two weeks. I don't know whether you could do that without this new technology exactly that way. So I think that there are some new wrinkles in the wine bottle, and we will leave it up to our other speakers to elaborate on those, but I think this is a new thing.

MR. HARWOOD: Okay. Thank you.

Our final speaker then this morning -- or panelist is Mark MacCarthy. Mark is the Senior Vice President for Global Public Policy for Visa.

And, Mark, I believe you have a brief Power Point presentation also?

MR. MACCARTHY: I caught the word brief.

Thank you very much. I'm glad to be here, and I thank you for coming all the way up here to listen to our discussions. And our host, thank you for having us here, and Julie and the Katies who put everything together, thank you all. I think this is a great show.

And I'd like to thank especially my son, Collin, who is on the sort of victory lap with me here. He just graduated from high school, and we're out here
in Seattle and San Francisco to sort of have a little
day off together, and I'm glad he came to watch me do
the show. He's a little nervous about all the lawyers
in the room. I told him that he should also be nervous
by the economists. They're also a threat to the common
man.

So let me just do a couple things. On the
slide presentation, you've heard a lot of this stuff
already and I'm going to jump to it pretty quickly. I
want to do some stuff on the business and what it's all
about. And then the material that we heard about, the
communications from Jennifer, I think, is really very,
very important.

I want to share with you what we communicate
with our issuing banks for their use with the people who
actually get the contactless cards, what we try to tell
them about the privacy and security issues, and then,
you know, go into some of the details that were raised
by some of the commentators so far.

So you can see up there the way this thing is
supposed to work. You've got a step where you take the
card, you wave in front of the reader. It does the job
that it's supposed to do.

The key thing that consumers have to know
about this -- and this is why I'm pretty interested in
some of the things that Jennifer has found out about
what consumers are thinking, even though the sample size
is small. The key thing they have to learn is how to
hold the card. Really, do I point that thing? What do
I do with this thing? And so one of the key messages we
have to get to people is how you hold the card in order
to make it work.

As you can tell there, it does -- the reader,
when it receives the information from the card and
processes it, it does beep or flash or sometimes both so
the cardholder knows that the information has been
received and the transaction has been processed. So
that's what it looks like.

Our business stuff -- just like Jodi was
pointing out, this is a business that's growing. We
have a momentum. 21 of our issuers have the contactless
programs. We've got a national marketing plan.

Some of our numbers -- partially in response
to Jean Ann's point about people going broke using their
contactless card, three-quarters of our transactions are
under $25. The places where people use these cards tend
to be places where it's low value, not high volume, not
high-value transactions. There is an increase in the
number of transactions. You can see the numbers there,
and there is an increase in the ticket size.
So those are the points that make it valuable for the merchant to use the program, and it's for that reason that we're seeing top merchant acceptance in the United States growing pretty dramatically. Here are the companies that we're working with and that have been picking up the contactless card at the point of sale.

It's not just the United States. Just as in MasterCard's circumstance, it's a worldwide program. We have programs all over the world, in Asia Pacific, Canada, Latin America, and Visa Europe as well. So this is a program that is not just in the United States. It's something that we hope to make a seamless, integrated global product, not one that's located in a single region.

I promised you communications that go to our cardholders in this circumstance. This is what we say: Visa payWave purchases are secure. They're processed through the same reliable payment network as the traditional magnetic stripe transactions.

In addition, the cards have special security features, and here's what we say about these security features: You keep control over the card. You don't hand it somebody else. Second, it's got to be really close to the reader. It's got to be within two inches of the reader. Again, that's partly security, but it's
partly just to inform them how to use the card.

There's special encryption processes. Jodi made reference to some of them. We'll talk about them a little bit more. And, of course, there's the zero liability. So we reassure the customers at the point that they get the card that there are security features in place that would protect them.

I was on the zero liability. I can't help it -- I mean, I think sometimes you just don't know what to say. But, you know, when we offered zero liability for all the transactions on our network, then the criticism comes back, but you don't offer protections for the transactions that are not on your network. How could we? So we do zero liability in the context of transactions for which we are responsible.

On a more general point, by the way, about consumer protections being embodied in law and being generalized to include all of the payment mechanisms, we agree. We have no difficulty in equalizing the consumer protections across the board and expanding them to all providers of payment services.

So if there are mobile payment devices that don't have those kind of protections -- I've talked to Susan Grant about this kind of stuff before and other people, and we would be very, very pleased to work

For The Record, Inc.
(301) 870-8025 - www.ftrinc.net - (800) 921-5555
together to put in place something that protects all consumers across the board. All right. That's our consumer communications.

Charge-back rules. The relevant feature here is that there doesn't need to be a signature, and the customer isn't required to receive a receipt unless he wants it. The signature, just to respond to the point that was made earlier, that's a protection really for merchant. The merchant has to prove that the transaction took place. And the signature is not to protect the cardholder, but to protect the merchant.

It's an interesting fact and maybe something that we should do something with that some other people in the study thought that the security that was provided by the signature was protecting them and, therefore, it's a useful piece of information to take back to our people in terms of understanding what people think about the security measures that take place at the point of sale. So those are our charge-back rules.

Risk assessment. There's a little bit time here, I think, to pause and give you a little context here. We do risk assessment all the time. It's one of our major things that we do in our business, and we do this for a very good regulatory reason and a very good business reason.
The regulatory reason -- I think, JeanAnn
made reference to this -- is that for reasons that were
good and sufficient to the United States Congress back
in the '70s, essentially a public policy decision was
made to put the risk of unauthorized transactions not on
the cardholder. I mean, there are details of about $50
and debit versus credit. But the fundamental decision
was made somebody in the payment system has to eat the
unauthorized losses. Fraud doesn't get put on the back
of the cardholder.

What does that is create a huge incentive on
the part of the payment system to get it done right, to
minimize those fraud losses, because they can't simply
pass them on to the people at the end of the consumer
chain. They have to find some way to minimize them, but
they pay those losses.

Now, over time, we've done our best at Visa,
and MasterCard has done their best to try to reduce the
amount of fraud for that regulatory reason.

The second reason, of course, is if there's
too much fraud in the system, then people lose trust in
it. It's not a trusted, secure operation. People say,
I've given you information and what have you done with
it? You haven't protected it, and I'm not going to use
your system. So we've got enormously good business
reasons to try to figure out how to do this kind of stuff right. That's in general.

In the context of contactless payment cards, we have an even further incentive. One of ways this product is going to succeed in the marketplace is that people believe it's safe and secure. And so we do not want to create the impression among people that by using their contactless card, they're creating an extra risk for themselves.

So we've looked at the kind of difficulties -- I'm going prompted by the monitor to wrap up. But we look at the kind of the difficulties that could take place in this area, and we're going to have some extended discussion about this throughout the day. So I just want to flash this up here and show you the kind of risks that are involved. And I'm not going to talk at this point about the details of these risks, the unauthorized card read, the eavesdropping, the relay attacks, the replay attacks and so on.

But I want to get to a detail that I think is really important, and I may go beyond this minute because I do think we need to get this fact out on the table if we're going have a decent discussion about the security issues.

Jodi made reference to what she called Dynamic
Card Verification value. We have a similar program in place to protect information that's part of a contactless transaction. But to understand it, you have to go back a little bit, and this is what's going to take me the extra minute.

When you have a regular transaction right now, a magnetic stripe transaction, the information gets passed through the Visa network. It's the cardholder number, the expiration date and a special security code, which we call the card verification data.

Now, the key fact about that is that it's a static number. And the way it works as a security tool is the card number is basically routing information, and the CVV is basically an access number. So the card number gets you to the bank that's involved, and then the bank looks for that CVV. If you've got the right number, they say, okay, you're authorized to gain access to this account. If you don't have that number, if you have no number at all or if you've got the wrong one, they don't give you access to that account. That's the security feature. It's a static authorization mechanism.

The new thing that's part of our contactless authorization is that that number changes with every single transaction. So if you do get the number through
one of these hacks, you can't use it again for a
different contactless transaction. That's the magic.
We made that number change with every single
transaction. We think that addresses a large number of
the security issues.

Security, of course, is not static. It
doesn't reach a point where we say, we've fixed the
problem and so we don't need to think about it anymore.
Our ongoing monitoring efforts haven't revealed any
excess fraud associated with contactless transactions.
So we don't think the situation we've got now poses a
significant security risk, but we're moving forward to a
new global contactless specification.

It's an upgrade to the way we do the process
right now. And as part of it, we're going to have an
additional security mechanism that you should know
about.

The additional security mechanism is that
right now when the card is brought within the range of
the reader, the reader energizes the card. There's no
new -- there's no information coming directly from the
card without it being energized by a reader. And then
information comes back from the card to the reader and
through into the system.

The new specification that we're putting
together will require that the readers will first send

to the card an unpredictable number, which will then be
used together with the information on the card to
generate a dynamic number that will change with every
single transaction.

The new thing here is that if you do get a
number right now from a contactless card, you read it
and you could take that number and route it through the
system and actually make one transaction. You couldn't
make two transactions, but you could make one.

Under the new specification, you couldn't even
make one because the card wouldn't have the number that
would be unpredictable and would come from the reader.
That creates an extra layer of security. It's the kind
of thing that will make it even more difficult for the
fraudsters to move ahead to make unauthorized
transactions possible with this kind of information.

This is a process that we're putting into
place. It isn't in place right now. The migration path
calls for card issuers to begin to put this into place
in 2009, and the mandate is up by the beginning of 2012,
that particular security feature be put in place.

Sorry to go over, but it was the kind of thing
that I thought we needed to get out here so people had a
full understanding of the kind of issues that we're
dealing with.

The last slide -- let me just leave this here. People talked about the form factor and how it's -- we're moving away from cards. It really is an important feature of this technology. And I know we're talking about security features. I know we're talking about privacy features, and those are important issues to focus on, but one of the things that this technology does is create the opportunity for moving away from the existing generation of cards and moving not just to cell phones or FOBs, but to any number of devices that could be used to embody payment mechanisms.

It's really an exciting development in the marketplace, and we're hoping that as it goes forward, it's the kind of thing that we can work together with people and the consumer groups, in the academic community and at regulatory community to sort of push together to make this kind of transaction work as well as possible for consumers, for the issuers and for the card --

MR. HARWOOD: Thank you, Mark. Thank you. Jodi, do you want to add -- do you want to add one quick comment? And then we have time for a couple questions.

MS. GOLINSKY: I'd just like to make a comment about zero liability. You know, MasterCard takes the
same view that Visa does. You know, one of the things that becomes very confusing -- and I'm actually a regulatory attorney and I get confused between Reg E and Reg B and what they have and what they don't, which is why MasterCard has a zero liability policy.

And Jean Ann did reference there are some restrictions on that; one of them being the number of times a year that a cardholder might actually make a claim of unauthorized use. That's meant to make sure that a cardholder is not abusing our zero liability policy.

But I manage that policy, and also I talk to issuers all the time who are the ones that mandate that policy for. And I've never seen a situation where a cardholder who's had an unauthorized use on their card and wanted to take advantage of the policy was turned down for reasons because of the limitations. Limitations are meant to make sure that there's no fraud to that.

On one quick point to what Mark said, the unpredictable number piece of their Dynamic CVV is actually something that MasterCard's Dynamic's CVC3 has now. We have do have that unpredictable number.

MR. HARWOOD: So let me see if we have some questions in the audience. We have one right over here.
We'll start Susan Grant. We have time for about three questions probably.

MS. GRANT: I'm Susan Grant, Consumer Federation of American. I just wanted to ask a question about the enhanced security that Mark alluded to which is really great news. Would that prevent somebody from taking the account information and using it in some other way to make an online purchase or a purchase by phone.

MR. MACCARTHY: It wouldn't, to be direct. If the personal account number and the expiration date were obtained, that information can still be used by a fraudster to go online and try to make an online purchase or do a mail order or telephone order purchase. Those are the contexts in which they don't need the card if they've got the card number and the expiration date.

Now, we think that that by itself is an issue that has to be addressed, but the card-not-present fraud is the kind of fraud that isn't going down as fast as we want it to go down. We need to address it with a series of general issues, general measures. We've got some things in place right now.

Most merchants, if they're worried about fraud in their context -- and they should, because the responsibility for fraud is theirs. The liability for
online fraud rests with the merchant. So they have got
every incentive to do this right. We've given them
tools to help out; one of which is the Card Verification
Value 2 on the back of the card. Merchants who ask for
that would be fully protected in this context.

   In the contactless card, the Card Verification
Value 2 is not on the chip, it's not on the magnetic
stripe. The only place you find that number is on the
back of the card. So if somehow the personal
identification number and the expiration date were
compromised in a contactless context, you still wouldn't
be able to use that number at a merchant. You used the
Card Verification Value 2, and almost all of them are
beginning to do that because they see the value of it.

   It's an address verification service that we
offer for online merchants who want to use it where
they'll say, what's your zip code. Again, that number
isn't present in the contactless transactions. So
there's no way the fraudster could use that.

   It's verified by Visa, which is a program
we're offering for the merchants, where if they do it
and they put it in place, there's no way that the
cardholder information that was compromised in a
contactless transaction could be used to get that
information.
And we think some of the merchants are really stepping up to try to take their own measures to protect fraud in this area. I mean, many of them use, you know, their own fraud screens like finding IP addresses that are suspect IP addresses, and they'll decline the transaction even in the context where the issuing bank would approve it.

So there are a lot of methods that are being done here to try to control online fraud. That's a very general problem. It's not a problem that's specific to the contactless environment.

MR. HARWOOD: Jodi, do you want to add anything else to that?

MS. GOLINSKY: I would say all the same things. You know, it's interesting because we -- at MasterCard, we have different terminologies. CVV, we call it CVC, whatever, same thing. Most online merchants are now asking for CVC too.

And, also, we have another -- we have a program similar to Visa's called Secure Code, which is a PIN system on the Internet if merchants want to sign up for that. But if you're looking to commit mass fraud online, trying to get numbers off of contactless cards is not your way to go.

MR. HARWOOD: Samantha, we've got someone back
there? Great. Next question.

MR. JOHANSEN: Hello there, Eric Johansen. As credit skimming is one of the most prevalent forms of fraud. By some estimates, it's a $100 billion problem that you guys are trying to solve. Current contactless systems do not address this issue, but you guys are talking about new security features that can help prevent contactless skimming. As you guys deploy these systems, are you planning on reissuing all the defective cards you have on the market today?

MS. GOLINSKY: First of all, we aren't the ones who issue the cards. But what MasterCard has done is we set up a mandate. I mentioned that we are mandating that all cards now do not have your name embedded in the chip. That was a mandate as of last summer. The mandate for Dynamic CVC3, which includes the unpredictable numbers is a mandate as of July of this year.

And then for cards that are already out there, we have a grandfather provision so by the end of -- and I can't remember if it's 2009 or right at the beginning of 2010, any card that's out there has to have been replaced by that time with the new technology.

MR. HARWOOD: All right. One final question. We'll go back there. Sorry about that.
MR. KOSCHER: Carl Koscher. So one thing that I've been wondering about is one of the nice things about the contactless cards is you can keep it in your wallet and still tap it against the reader and it will work. So I'm wondering once issuers start sending us cards and we have a wallet full of cards with these PayPass features on it, what happens then? Does one of the cards get randomly chosen? Are consumers being informed about that?

MR. MACCARTHY: My answer is that they interfere with each other, and so the result would be that you would have to pick one.

MS. GOLINSKY: And one of our strategies has been to -- you know, some cards you want to -- your marketing strategies try to get various cards in someone's wallet. For the PayPass, you just want the one in your wallet.

MR. HARWOOD: Are you going to ask a follow-up question?

MS. REDFORD: Leann Redford with Visa. So what you're saying is if you have multiple cards, how do you pick the one at the point of sale, because it has to be awfully close? So you're the lucky consumer, you're holding a whole handful of -- you might say a whole deck of cards in your hand, and you hold them towards the
reader. Our technology specifications say the reader can't choose. We know what card we'd like you to choose, but the reader doesn't get to choose for the consumer. So the terminal says, whoa, I've got more than one card in the field, please stop and have the consumer choose which card they choose to pay with, debit, credit, brand, whatever. Does that make sense? We could technically solve that problem in our favor, but that's not part of consumer choice.

MR. HARWOOD: Thank you very much. Thank you. We're out of time. I apologize we didn't get to this last question here. You're welcome to come up and chat. We're going to take a 15-minute break. We're running a few minutes late. So it's going to be a definite 15-minute break, not a 15-and-plus break.

And the folks who are in the next panel, if you could come up in about five minutes and meet with Julie, she'd like to see you before we start. Thank you.

(Recess taken.)
CONTACTLESS PAYMENT CARDS

MS. MAYER: We have good information to share on this panel, and I think the discussion benefits from the previous two that we have heard, about how contactless payment technology works, how it's being used, discussion of consumer attitudes and understanding regarding contactless payment devices, and now we're going to focus on this panel on one specific form factor medium, plastic cards, payment cards.

Our panelists all bring great expertise to this discussion. At the same time, they offer, I think it's safe to say, diverse perspectives on the benefits and risks of contactless payment cards, and we're pleased to have such a range of stakeholders represented on this panel, including payment card issuers, users, and skeptics.

We'll also hear from experts who have consulted on security and regulatory matters from members of the contactless payment industry, government, both in the U.S. and in Asia, where contactless payment is arguably even more advanced.

One person we won't be hearing from, unfortunately, today is Leslie Michelassi, who is on the agenda, who is the Financial Consultant and the Washington State Director of CASPIAN, a consumer privacy
organization, who unfortunately was unable to come at
the last minute.

However, we will start with Peter Ho, at the
far end of the table, and Peter is Vice President and
Product Manager with Wells Fargo Card Services.

MR. HO: Thank you very much, and I
appreciate the opportunity to speak in front of everyone
today. As I've been introduced, my name is Peter Ho, I
am a vice president, Product Management, in Wells Fargo
Card Services. That is the consumer payments wing of
Wells Fargo Bank. We are an issuer of Visa's payWave
contactless card feature, both on the credit and the
debit side. And I'm here today to really share our
perspective on why we are issuing contactless cards and
where we see the market and where we see the trends
going in terms of contactless payments.

Just to kind of high-level start off, at
Wells Fargo, our philosophy really is, we want to be our
customer's payment of choice, and it doesn't matter
whether you use Wells Fargo credit card, a debit card,
or one of our gift cards, but what we like to do is we
like to take advantage of the relationship that we have
with our customers, and we like to show value as a Wells
Fargo relationship versus any single product.

Part of that strategy are payment cards;
they've become a very crucial part in our lifestyle.

People use both types of cards for -- all three kinds of cards for their payment needs, and they've really become a great aid in terms of conducting transactions.

Key to, I think, this ability is the quick, reliable networks that we have, so that when you swipe your card, you know that that transaction is going to go somewhere, you're going to get an approval, or, unfortunately, sometimes a decline, but that happens very quickly.

It eliminates the need to carry large amounts of cash with you, so it's a personal safety issue, right? If you're going to go buy that big screen TV, you don't want to walk around with a couple thousand dollars in your pocket. The value proposition to the merchant is the same thing: You don't want your cash registers full of cash. It's a huge risk and liability in the sense of, God forbid, a robbery.

Also, international acceptance. Cards are accepted worldwide today, and instead of having to work out and have foreign currency, hard cash in your hands, you can basically take your Wells Fargo Visa card, go overseas, use that card seamlessly for any purchase you need to make.

And lastly, I think, there are benefits to
having a card, in terms of chargeback feature, extended warranty, and other value-added services that we add.

When we get down to contactless cards, this really is an extension of what it is that we currently do with our customer base. This is designed basically for small transactions, transactions under $25. I think Mark did a great job in explaining some of the regulations and how this $25 transaction limit -- and it's not really a limit as much as this is where a merchant is protected, and for the merchant who wishes to go above that $25 without a signature, they certainly can, at their own risk, and some merchants have decided to take on that additional risk and others haven't.

So depending on where you're shopping, you may or may not be asked for a signature. It is an inconsistent experience, but at the same time that gives the merchant the capability of making decisions on their own.

It also provides speed in terms of you can just wave your card; you don't have to worry about orienting your card based on the different kind of terminal that you have there, and I'm sure you've been stuck behind somebody at a grocery store waving their card six ways to whenever, to try to figure out which way is it going to swipe for me, or is my card
demagnetized.

Also, convenient. Contactless payments provide an opportunity to actually allow us to meet the lifestyles of our consumers in the sense that we can introduce other form factors that may be more convenient. And I think a lot of people today have spoken about mobile, of which we are very keen on, and I think Mark put up a slide demonstrating the various Visa form factors, including the mini card and the key tag.

Lastly, it's a security feature, in the sense that you have control of your card at all times. I think a lot of people mentioned today skimming, and skimming is an issue. And what happens in skimming is, someone takes your card, whether it's that server at the restaurant or a clerk who actually drops your card onto the floor, picks it up, swipes it into a machine and comes back up and gives it back to you. Bottom line is, they are stealing information that is based on your payment card. In the case of contactless payment, you always have the card in your possession, you don't need to give it up.

So getting into customer communications, I think a lot of people have talked about customer communications and what are issuers doing to communicate with their customers that they indeed have a contactless
card in their pocket.

So what I did is I went ahead and ordered a contactless plastic from our founder, Henry Wells, and typically you'll get, you know, you probably recognize this kind of envelope in your mail when you get a new plastic card, and inside this card, we have a number of different pieces. First and foremost is what we call our card carrier, and as you will see, it's basically your standard card carrier. On the card itself, you notice at the very top we do say, you know, same great card, new payWave feature.

And underneath the card, actually, if you tear the card off, it actually says, introducing Visa payWave, and tells you what exactly this card is and what it does.

At the same time, in addition to the card carrier, we also have a brochure introducing Visa payWave. And in this brochure is a lot of the similar messaging that Visa has helped us define, and basically it provides information on how you use your card, how you identify that you have a contactless card, and, most importantly, where you can use it or how you find out where you can use it.

So that's information there. In addition, we have to include all of our other pieces of information,
keeping your information safe, and our card disclosures. But at the end of the day, there's a lot of information in this package, and it does tell the customer, yes, you have a contactless card; and that's great, but the one thing to keep in mind is, in our studies, only ten percent of the people read the stuff in the envelope.

So as much as we do our communication job, we still have to depend on the consumer to read the information we give them. And if we can't, you know, there's nothing I can do. You know, I can't go around bopping people on the head saying, hey, are you aware of this? But I think we've done a great job in pointing out the features in having this card.

In addition, if you notice that this card itself actually has kind of a silver metallic label on the top; it's the activation label. Actually, this is a security feature that is a mandated Visa, we call it, shield, the card shielding in the mail stream. What this does is, it actually disables the contactless feature of the card until this label is removed.

So the concern is, if I send out a bunch of cards in the mail, and, here, I'll just put this back into the envelope, and somebody in the mail stream decides, hey, I'm going to read a bunch of cards today, well, this is an actual contactless reader. I've waving...
the card all over it. It's not reading; it's not beeping. And just to prove that again, I'll go ahead and -- (Demonstrating). It's not reading. It's to protect our customer.

The moment this label is removed, though -- and I'll go ahead and remove it -- the card reads.

So what are we doing to protect our customers? What are we doing to show our customers that they have a contactless card? The information in the packet, bug on the card itself, demonstrating that we do have a contactless feature, and in the mail stream we protect it.

In addition to that, from day one, we've been issuing cards since August of 2006, we have used dynamic CVV on all of our cards. We have also masked the name on all of our cards. What that means -- and I think we've touched on that earlier today; what that means is, basically, your name is not populated on the chip. Instead, it says Wells Fargo card holder. And if you'd like to come up later on, I do have a few receipts showing that printout. It's a little yellow, and I apologize;, I've gained a lot of weight testing out this thing at all the fast food restaurants, and so my girlfriend said I have to lose weight.

Anyway, but getting back to the point here
is, we are protecting our customers, and we are
protecting our customers in many different ways, and the
card is a secure card. When you look at how someone
could steal this information, and the one thing that we
have to think about is, when you steal information,
that's one thing, but what can you do with the
information you have is a whole other case.

If you were to take this card, or even if you
take the card in my wallet, and you were to get that
information off of it, what would you get from that
read? You would get my name field, which would say
Wells Fargo card holder on it; you'd get my account
number and expiration date, the dynamic CVV of the last
transaction that I used the card for, which was this
morning to buy coffee.

If you were to take that information and you
said, okay, I'm going to clone myself a magstripe card
so that I can go and fraudulently buy gasoline; well,
the thing is, that can't happen, because in a magstripe
transaction, as Mark alluded to earlier, you need to
have something called CVV1, or MasterCard is a CVC1. So
basically, when you try to swipe -- when you take my
DCVV value and put it into the CVV1 slot in this
magstripe, it will decline, because it won't match.

So then you say, okay, well, then, I'm going
to make a bunch of fraudulent transactions on the Internet. And as pointed out earlier as well, that can be done; however, many consumers are -- or many merchants are actually starting to use CVC2, which basically is this three-digit number on the back of your card, right? You can't read that wirelessly. It's not on the chip.

So the last option really is, I'm going to go try to clone myself a contactless plastic. And I'm not going to say it cannot be done, because we all know that things can happen over time; however, it is a very difficult proposition today. You have to get the algorithms right, and it takes time to get that done, and it takes expense. It's a lot easier to go find other ways to create fraud other than the contactless feature.

So getting back to talking about security, I did read a lot of the comments in the comments section, and one of the things I did notice was a lot of people were saying we should have more security around these cards. And I would say, yes, that does make a lot of sense; however, we also have to think about the fact that we are working within an ecosystem, and this ecosystem includes merchants and it includes issuers and it includes consumers.
The more difficult you make something -- or
the more secure you make it, usually it means more
expense from the merchant's point of view, because
you're adding additional security features that cost the
merchants in incremental cost, it costs the issuer
something, and at the end of the day it also costs the
customer something, because they have to learn how to
use the card.

And so I think we're walking a fine line, and
I think we've -- we might be tipping on one side or the
other, but we're definitely not one-sided in terms of
the security features that we built into this program.

And so going forward, I think that we do have
a very, very bright future for contactless payments. I
think that cards are really just a beginning for people
to think about what it is that contactless payments can
do for them. I think at the end of the day, something
like a contactless phone will actually offer more
benefit to a customer, and they will have that choice.

I mean, this phone here, it is a contactless
payment device, and basically I have the option of
setting this phone to make transactions based upon three
levels of security.

The first one is basically no security,
always on, so I just walk up and I tap the phone, it
will read -- it is reading, actually; it's just not beeping for me.

The second level of security is you have to actually go into the menu structure of this phone, find the application, actively say, I want to pay, before you can pay.

And then lastly, you have a feature that basically locks it down with a PIN, so you can't do anything with this unless you'd have a PIN to activate.

Lastly, the nice thing about contactless applications on the phones is, the phone and the payment application can be disabled from a remote location, something I can't do with a card.

So the future of contactless payments is very bright. I think that there is still a lot of education and a lot of understanding with consumers, no doubt about that, but I think the more and more consumers start understanding the wave as opposed to the swipe, we'll start seeing much more attraction and understanding and use of contactless devices.

And I'm getting my signal, so I will go ahead and say thank you for your time. I applaud the FTC for putting this program on, and I'll be available for questions later. Thank you.

MS. MAYER: I have one question for you
before you sit down -- or you can sit down.

    MR. HO: Thank you.

    MS. MAYER: I just was curious how Wells Fargo was targeting -- if this is going on, targeting which customers were receiving these cards and getting these disclosures in the mail, or it was something driven by if consumers were asking for them as well.

    MR. HO: That's a really good question, and we actually have a multi-pronged strategy in getting contactless cards to the customer.

    The first one is, if you're a new customer and you're applying for a new account, the contactless feature is a choice that you can select. So you can have one mailed without the feature, one with the feature.

    Also, what we call natural reissue. We do reissue cards, a number of them with the contactless feature, based upon some segmentation that we do and to customers that we feel would benefit from the feature. They still do have the option of opting out of this, if they so choose, by calling customer service, and we'll have a card out to them pretty quickly. In the meantime, about six, seven seconds in the microwave on medium. No more, no less.

    MS. MAYER: Thank you for that tip.
Next, we're going to hear from Dan Johnson, who will represent one of the retailers, particularly in this area, with Tully's Coffee, which many of you are enjoying this morning courtesy of the cafe. He can speak to how long they've been using it in their retail shops, but it's also interesting to hear again their reasons for doing so, and experience since, and Dan is the Information Technology Director for Tully's.

Take it away, Dan.

MR. JOHNSON: Thank you, Julie. And thank you to the FTC for having this. I think this is a great opportunity for a good knowledge transfer from various experts, and I'm happy to be here.

I'm going to keep this pretty short, really. I'm going to go into kind of the facts a little bit about the company, about why we decided to go with contactless payments and our results so far, but really if you have any questions, I think that's going to be the best tool for getting information from me, is what questions do you have about Tully's, and we can do that afterwards, or you can come up and see me afterwards, definitely.

A little bit about Tully's. We were founded in 1992 by Tom Tully O'Keefe. If you're not familiar with our brand, we are a custom, hand-roasted coffee
company. We do everything by hand; we don't use machines; we have people up there sniffing coffee and abstain from technology on that side of it as much as we can, but also from a retail perspective, we obviously embrace it as we need to do business.

We have 150 retail locations domestically. Of those, 90 or so are corporate locations which are using contactless payments. The others are franchise locations. Additionally, in Japan, we have over 250 franchise locations. We just started up a company in Singapore to open coffee shops up there. In addition to the retail, we also have grocery stores; we're in over 4,000 grocery stores across the West Coast.

We're going to be focusing on the retail side. The retail side of our business is pretty straightforward, and we sell coffee. I saw a lot of people out here drinking it this morning. We are the official coffee of the University of Washington Food Service. We have a lot of other areas, including Boeing, and we're hoping to expand east farther.

But in retail, there's really, and especially not just retail, but QSR, quick service restaurant, there's three big drivers on how successful we are.

The first is quality. You have to have a good quality product, which we believe we have. We
wouldn't be in business if we didn't have a quality product.

The second is value, and that could be either perceived value or actual value. You know, compared to some other coffee companies, we have a great value for the quality of coffee that we have.

And really the third big driver is convenience, and that's really the big one. Convenience is probably the easiest one to really communicate and really touch with our consumers.

Convenience can be multiple things. It could be store locations. There's a very big coffee chain based in Seattle that has them everywhere, and they have been relatively successful, although I think they're just recently closing some stores, so maybe that's not as convenient as we thought it was.

In addition to location, you have speed of service, and that's kind of where contactless comes in. People, especially in the morning, and coffee, we do 60 to 70 percent of our business before 10 a.m. in the morning, and when you're there, there is a line out the door and you need to get them through as quick as possible.

So really from a convenience perspective, we kind of started looking at the contactless, saying, is
it something that we can use to speed up our line? Will people who have contactless cards not order the super-double-tall-nonfat-soy-chai-latte-no-whip and not hold up the line trying to figure out what they want to drink?

But seriously, looking at the contactless, we said, you know, we need to look at a couple things.

One, electronic payments make up over 50 percent of our revenue stream right now, so we are still primarily a cash business, or equally cash and electronic, so we need to make sure we accommodate both, but we are only going to be seeing an increase in electronic payments, and whether those electronic payments are gift, credit, or contactless, we need to be sure that we capture or have the ability to capture all of those.

Also, from speed of service, the guise of contactless is that it does make it go faster, that there is no fumbling through the wallet for the card, and that was intriguing to us and hoping that it would speed up our service.

Also, it's an option for our consumers. We found some consumers have come up to us and said, hey, I have this great, nifty tool; can I use it at your store? And although that itself isn't necessarily a driver, I
don't think we're turning away customers when they come up to us and say, oh, I'm not going to use your shop because you don't have it. It is another option for people that are very passionate about that and who do want to use it.

The other driver for us, as mentioned, is for people to spend more money. And I will put a little asterisk by that and say we don't really want people to spend more money; we want them to spend more money at our shop. So again, if it's a convenience factor that we can get them to come here and spend money at Tully's instead of at a different coffee shop, that's perfectly fine with us. So we're not out there to bankrupt the public; that's definitely not our goal.

The implementation of this, we kind of started going through the process about a year and a half to two years ago, after we made the decision to go on it, and really we took a look at all the business factors for doing it. We looked at the costs of doing it, which they were not significant, they weren't not significant, but it was a risk that was relatively low. It was something definitely that we could tolerate.

So we did a pilot in five locations, and that worked out very well. We use a Verifone Omni 3750, and actually the ViVOtech reader that you see in front of us.
here. Installation was pretty quick. It was pretty cheap. And from a point-of-presence perspective, it does kind of stick out in front of the register, and we got a lot of questions when we first put them in saying, hey, that's great; how do I use it? I can't tell you the number of people that don't have contactless cards that try and use that reader. It's a constant problem. But that's neither here nor there, and I'll actually get to that here in a little bit.

After doing the pilot for four months, really that was just to see if the technology worked. The biggest thing we wanted to make sure was that adding contactless didn't disrupt our credit card processing. That was the main driver. Is this something that we can offer that's not going to risk any of our current streams? So after determining that was the case and we had some usage of that, we went and rolled it out companywide.

And getting to the results section, first of all, I have to put a little PCI disclaimer, which says that we don't save credit card numbers. Tully's does not save any of that. We know the banks do. We don't have access to that, so I have truncated data. So I've got a bunch of numbers that have the last four digits, and trying to figure out frequency, recurrence of
consumers. So it's not accurate, I can tell you that, it's not 100 percent accurate, but it should be ballpark in terms of what we're seeing in terms of repeat customers, who's using it, and why they're using it.

MS. MAYER: And I'm just going to jump in and say, for those of you who don't know about PCI, we'll be hearing more about it in two presenters.

MR. JOHNSON: So what we saw is that people that do have their contactless cards and do use them actively, always use them. There's a small percentage of our overall credit card customers that use them, but those that do have the contactless cards do use them. And I don't know why, I don't know if it's they think it's really cool, they impress the other people in line by pulling out the contactless card, they're impressing our baristas, I'm not sure exactly why they're doing it, but they are consistently using that card. It could also be that there's rewards or other aspects put onto that card, but that is their top-of-the-wallet card.

Overall, as a percentage of credit card customers that are using contactless, it is very, very small still. It is a very, very small number of people that are using contactless cards as opposed to regular magstripe cards. And part of it is the saturation of the cards out there. A lot of it could be, again,
different rewards that people have on cards that they haven't been offered as contactless yet, but we're expecting that to grow, but it is very small right now.

I put a little note in here; some of the other issues we've had, especially with this reader here and people that don't have the contactless cards is, we have to remind people to tap or wave and not hit. We've had several readers damaged, especially people with the noncontactless cards, they try and use them and they say, oh, it's not beeping, so they keep on tapping it harder because they think that's going to make it read better, which is actually quite humorous and has resulted in damage to some of our readers and cash registers.

So really, that's about it in terms of the results. We see that there's a lot of potential for it. There's a lot of potential for getting this into people's hands. There's a lot of potential for the mobile application of this coming up very soon, we hope. We think that it's going to do very well in that.

As it is now, it's not a big home run. It's nothing that is going to significantly drive our business currently, but also I would expect that to incrementally change as we get more people out there having these cards, as there's a greater education about
these cards, and as we put on additional, maybe, marketing aspects of that to get people to come in.

So overall, it's a program that has worked well for us. There's really no negatives. We received no customer feedback, comments, about this in the negative. We've had no chargebacks related to this. Obviously, we wouldn't be liable for them, anyway, but we haven't had anyone actually challenge a contactless transaction.

So overall, it's worked very well for us, and we look forward to the future and hope that this does really turn into more of a convenience factor for our customers and get them to come back more frequently.

MS. MAYER: Dan, I just have one question. I asked Peter a little bit about education, and I'm just curious if barista education or employee education is part of the retailer's responsibility, because, and not necessarily in your stores but in others, now that I've learned a lot about this technology, I've been asking about it: Oh, you know, how do I use this, or what's this? And I often get the "I don't know," so I'm just curious if that's part of the merchant's role in getting this technology out.

MR. JOHNSON: Yeah, it definitely is. I've got to say, you know, MasterCard, Visa, and AmEx have
been very helpful to us in terms of giving us materials
to use to help train our baristas on that. We do have a
relatively high turnover in terms of staff, so getting
people on top of that can be sometimes problematic, and
we do our best with that, but definitely there is a
barista education there that can take a little bit of
time.

It's kind of funny, because contactless
payments are supposed to be quicker, but a lot of times
you'll have the person that pulls out their wallet and
they say, oh, I have this card and I'm not quite sure
how it works. And they kind of look at it and the
barista looks at it and says, oh, you know, let's see
how we get this to work. And overall, that transaction
was eight times longer than a typical magstripe, but you
hope that the next time, once they have that and they
keep on using the card, that education level builds.

But, yeah, definitely in the short term,
there are challenges with both education, awareness, and
consumer awareness of the tools that they have.

MR. HO: Just a real quick point. I think
the big thing there is, especially in the card form
factor, people are falling back on the magstripe, but
the moment you start going to alternate form factors,
like phones, like where there is no magstripe, suddenly
people really do need to pay attention.

I was at a local drive-in one day, and she said, oh, that doesn't work. And I said, well, here, I want to pay with my phone. She says, don't worry about it; I can swipe it. I said, all right, well, here you go; swipe away.

So education is coming, and I think, as I was pointing out earlier, as more and more consumers understand it, those consumers become the people standing behind the counter accepting your payment.

MS. MAYER: Thank you both.

We're next going to hear from Dr. Kevin Fu, who is an Assistant Professor of Computer Science at the University of the Massachusetts Amherst, and he also directs the RFID Consortium on Security and Privacy, which are topics we'll be discussing today.

DR. FU: I think it's great to follow Tully's. I love coffee, and I actually love their coffee. But I'm wondering about the reasons they actually have the customers using those contactless cards, whether it's actually to pick up the line or, rather, it's a pickup line.

MS. MAYER: It was just a happy accident that it turned out that you're the official coffee of the University of Washington.
MR. JOHNSON: And we're happy to be so.

MS. MAYER: And right across from my office.

DR. FU: Okay. All right, so when Julie mentioned the type of people on the panel, she talked about stakeholders, and then she said, oh, and then other skeptics, and I think she may have been referring to me. But I consider myself a technologist, because I'm not financially motivated behind this, but I'm curious about what is the security and privacy on these kind of devices, what do they do today, and what could they do.

In fact, I would love to be able to buy a perfectly secure mobile payment system. I enjoy this kind of stuff. I think it could be great in the future. But the problem is, there are many ways to actually execute it. And without the proper incentive systems, we may end up with the kind of technology that we would rather not have as consumers.

So what I'm going to do is, I'm going to give you a quick survey. There's quite a bit of material; you can find all this material on the RFID-CUSP Web site. But what I'm going to do is just tell you about one experiment I did on contactless credit cards. I started to receive these cards in the mail, and I was really curious how they worked and what
kind of information was on the card and what was revealed.

We had heard about, for instance, the Exxon Mobile Speedpass which used encryption to protect its payment technology, and we thought, wow, these contactless credit cards, they are years ahead of these other payments, so it's going to be really tough to crack, probably.

So what actually we found was, we didn't actually have to do too much in order to lift information from these cards. On these cards, we were able to -- we took a collection of cards -- I probably have one of the worst credit ratings; I made sure to buy my house first before doing these experiments. But we collected tons of cards and tried to catalog what information was leaked. And we took an off-the-shelf RFID reader. We also built one of our own. And on most of the cards, we could lift the credit card number, the expiration date, and the card holder name.

Now, I do congratulate the credit card associations and the bank issuers for beginning to remove the card holder name. I understand some of the cards are beginning to remove that. I think that's a great step, a good step in the right direction. I'm glad that they're sort of taking these preemptive steps
after the fact.

But let me give you a little video to
demonstrate what we actually did.
(The video was played.)

DR. FU: So that was an actual skimming
transaction. They added the stench marks to my poor
graduate student. But that was an actual skimming of
information. It was a blink of the eye. It was able to
read through clothing, through the wallet, through his
coat, and pull out his complete information on the
contactless card.

I feel like there have been a lot of
acronyms, legal acronyms, and so now I'm going to throw
you some technical acronyms, but I'll try to keep that
down.

But here's just a picture of one of the
devices we built that is actually able to replay
contactless credit card information, and we found some
interesting things despite the protections of things
like transaction counters. And I'd be glad to talk with
you about these kinds of devices offline.

A lot of people ask me about, how do they
disable the contactless interface on the card? Mr. Ho
suggested the microwave. That's fine if you like to see
sparks, I suppose. I get a number of phone calls,
though, asking me, how do I do this? They've called up their credit card issuing bank and they've asked not to have the contactless, an enabled one. And an interesting story came back.

One woman said she called up her bank, and they said, we'd be glad to issue you a noncontactless card. Came in the mail. She opened it up. Investigated a little bit further. It was actually still contactless. But she wasn't able to actually tell, because how could you distinguish these things, they're so pervasive.

But one way you can actually disable it is with a hammer, and so here I have a graduate student and he's -- if you hammer it just right, often times there's a little bit of an indentation and you can dislodge some of the leads and that will effectively disable it. You could go test it out, I suppose; if you take it to a store and if it doesn't beep anymore, you probably damaged it enough. But it's not something I would suggest to the average consumer. Don't take a hammer to your wallet.

Okay. So with that, I have a couple other nongraphical comments. Hang on one moment.

And it's mainly going to center around three issues, and that is of personal privacy, informed
consent, and consumer choice.

So it is my opinion in looking at these things as an unbiased researcher looking at these kinds of devices, that these kinds of devices could benefit from much more privacy preservation. So let me give you a couple examples.

There is a professor of electrical engineering, okay; this is your high-end consumer who knows not only how to do things but how they're built. He walked into my office, and I said, what kind of contactless cards are you carrying? And he said, are you kidding me? I wouldn't carry that. And I said, are you sure? And he said, I'm absolutely sure. So we said, okay, let's find out.

I had my student walk up, brush by him, and he said, guess what? You're carrying a card. And he said, no, you're kidding me; I'm not actually carrying a card. And he said, well, how did I get this card? And we said, well, we don't know; you must have gotten it in the mail somehow.

So we don't know what kind of information was provided to him, but apparently one of the most educated people with a Ph.D. was not able to comprehend whether a card was contactless or not. So that's just one data point for you.
One other interesting thing is about the card holder name. I'm really glad that the card holder name is being removed, at least from the consumer perspective, because the consumer then doesn't have to worry as much about their name being exposed wirelessly. I would be interested in hearing more about what that does for the other stakeholders besides the issuing banks and the payment associations.

But one interesting thing is, I was never notified that my name was either on the card or was being removed, and I'm still waiting for my notification to say, I'm sorry, sir, we had accidentally put your name on the card; we are removing that, and here is your new card. I have yet to receive any kind of notification of that nature.

On the topic of informed consent, I'm a strong believer that consumers need to be able to make informed decisions. In fact, earlier today on the panel, two panels ago, you heard from Mr. Vanderhoof that people should make informed decisions on how and whether to use contactless technology, and I agree with that. And I think part of that statement means consumers need to be fully aware of the risks and benefits, just not the benefits but also the risks, so they can make these kinds of informed decisions. So let
me give you another example of that.

A press release from Wells Fargo stated in June 2006: Visa contactless is enabled by radio frequency technology. The contactless RF payment chip uses industrial strength encryption technology, 128-bit and triple DES encryption, the highest level encryption allowed by the federal government. The chip contains the same minimal personal information found on a traditional magnetic stripe card, just the account number and the card holder's name.

Well, to me, even as a technologist, that implies to me, oh, wow, you're using encryption, so you're encrypting it. Well, then, why were we able to read all of this information off the contactless interface and discover no encryption protecting that at all?

So what does it mean when you say you're protecting it with encryption? What exactly does that mean?

It was implying, at least in my opinion, that strong encryption was being used to protect this kind of consumer information. But what it actually, I believe, is doing is protecting it in certain locations but not in all locations. In particular, it was not protecting the contactless interface.
Okay. The third topic I wanted to touch on was on the notion of consumer choice. So today I kind of make this analogy of, the choice of consumers is sort of like the airlines before the cost of oil got so expensive, and that was, today you have a choice of chicken. So today, the consumers have a choice, and it's hard for them to make that kind of choice, so how do they know what kind of card they're getting, for instance.

And there are two kinds of consumers who are going to care about this. One type of consumer is the kind of consumer who just deeply, fundamentally cares about their personal privacy. I have no qualms with that; if they want to remain anonymous, that's fine by them.

Another kind of consumer is one who might unknowingly carry a card. Maybe they don't care so much about their name being stored in some kind of database, but they'd at least like to be aware that it's being stored in a database.

And what I've observed is that neither of these types of consumers right now receive what I believe is sufficient information and customer service to make informed decisions.

So let me give you a couple more examples.
One example was what I consider a botched handling of an opt-out request. And again, this was actually the request I talked about; she called in and asked for a noncontactless card and she was issued a card that still contained the contactless. And one of the problems here was, it's very difficult to distinguish these kinds of cards. And these cards have to be distinguishable not just by Ph.D.s, like me, but they have to be distinguishable by the average consumer.

And the customer service, for instance, needs to be more well trained. I'm going to guess that there's probably been a lot of training going on in the companies, but I think that the service representatives still, kind of like the cashiers who use this technology, aren't quite aware of how it works themselves.

One example of that, I have an undergraduate from Malawi this year, and he's doing a project this summer on contactless, and I told him to play with it. And he said, oh, I'm really excited about it, so I went down to CVS and I wanted to use my AmEx, and the cashier swiped it. And he said, no, no, no, no, I want to use the contactless. And she said, okay, I'll swipe it again. Then he said, no, no, no, no, void that transaction; I want to use the contactless. So she
said, oh, okay, I'll void your transaction. And she tried to swipe it, and so she started inserting it into these holes, and she clearly did not know how to use the card.

So there is going to be a lot of education necessary, I agree with that, on both the merchant side and on customer service; otherwise, they won't be able to provide the customers with the kind of information they need to make the decisions that are important to them.

So in summary --

How am I doing? I've got a couple minutes.

So in summary, I think that these contactless payments, they could hold great promise. There's no question that it's going to speed things up, especially in situations like public transit, where you care about high throughput. But the problem is, there are other issues at play. There are tradeoffs and there are incentives, and the problem is, what are those incentives and how is that going to affect the things that are most important to the consumers instead of most important to the bottom line of a company who's issuing these kinds of cards.

So analysts have proven that proprietary systems from payment associations in the past have
failed to protect basic kind of information to the same
degree that you'll hear about in a moment on PCI.

There was an interesting comment at the
Federal Reserve Bank last year, where one of the
merchants stood up when I was talking about this
technology, and we were explaining how, yeah, it's not
actually encrypted going over the contactless link, and
he asked the question -- he was actually the fellow from
CVS, and he asked: Why is it then that you require the
merchant to encrypt all this information under PCI, but
the issuing banks don't have to do that on the
contactless interface; why is that?

There wasn't a good answer to that, but maybe
we'll hear about this later today.

So in summary, I think that consumers
shouldn't remain these sort of unwilling beta testers of
new technology. It's great that they sort of fix the
problems after, you know, some poorly paid professor
identifies and says, well, did you think about this?
And they say, oh, okay, we'll fix that. And then do I
have to come back next year and say, did you think about
this other thing? Oh, we'll fix that, too.

Or are they going to just have some kind of
overarching incentive to make sure they get it right in
the first place before this really takes off. Because
today, the technology is rather -- it's not as widely deployed as it will be, and when it is widely deployed, it's going to be way harder to fix these problems. When you move from 20 million to 300 million Americans, it's going to be much harder to fix security problems and privacy problems.

So in summary, contactless payments need stronger privacy and security mechanisms, and I don't think that the incentive mechanisms are in place yet to encourage the stakeholders to do this level of security.

Thanks.

MS. MAYER: Thank you, Kevin.

And I don't know if Peter or anyone wants to respond to anything specific that was discussed about, you know, what was in a press release in 2006. But one thing, to put that in a context of a question is, putting aside, assuming those terms as being used for your cards were accurate, if that tension between being accurate and disclosing everything and actually being effective at educating consumers, if they would understand what 128-bit encryption was, but I'm just curious if things have changed since then.

MR. HO: You know, I don't think anything has changed since then. I think basically the 128-bit encryption is built in to, as was pointed out earlier in
a presentation, the UDK keys; they're loaded onto the
card, and that is where the encryption is. And at the
end of the day, when you're looking at speed and you're
looking at being able to turn something quickly, you
look for areas where you can -- you don't want to cover
up the whole thing; you want to be able to get it done
quickly, and so that's where it is.

And at the end of the day, we released our
cards in August of 2006 with full name masking, with
full mail masking, following best practice. We never
issued a card with a customer name on it.

MS. MAYER: Thanks, Peter. I know there will
be questions from the audience, as well, when these two
gentlemen are finished with their presentations.

But next, we welcome Tom McAndrew, who is
going to talk about the often-referenced PCI, otherwise
known as payment card industry, standards, and Tom is a
PCI Qualified Assessor whose firm, Coalfire, specializes
in information technology audits, compliance, and
forensic services. And Tom, in particular, has worked
with a range of players in the contactless industry,
including merchants, service providers, and technology
manufacturers, so he really has a depth of familiarity
sort of from the outside on these issues that have been
raised.
MR. MCANDREW: All right, thanks.

So again, my name is Tom McAndrew, and this is definitely an interesting forum, I think, to go through this, because as you see, I mean, everyone has kind of got an agenda here.

So one of the perspectives that I would like to bring here is to make sure that there's an understanding what all the players are. And this is important just not for you consumers, but also, I'm guessing because of the building we're in, there's a bunch of attorneys here as well, and this is becoming an increasing area of litigation and responsibility and passing on liability throughout the industry.

So it's really important, because the fundamental consumer, an average card holder, doesn't understand what being compliant means; they don't understand who's involved; they don't understand what the fines are, how they get assessed, and ultimately who's in their best interest. So I just wanted to cover a couple different topics here.

I want to talk about what the ecosystem is between merchant banks, member banks, acquiring banks, card members, card holders, the PCI Security Council, so talk about that at a high level once we understand what is compliance and how is it being enforced and what is
it not covering.

Compliance is still kind of ongoing, as we see with Gramm-Leach-Bliley compliance in banking, HIPAA compliance in health care, there's a bunch of different areas out there and it's being enforced and supported differently, so it's important to kind of understand that and understand what the limitations are with contactless, because it's an emerging field, and as with all areas, the regulations are lagging behind where the technology is emerging.

Then talk about what the actual focus threat is. So what are we actually seeing out here? There's a lot of areas where we can see, you know, there's great videos out there, you can go on YouTube, you can see what people are doing, but what is actually going out and quantify what some of those risks are.

And then last, kind of talk about the current stage today with contactless and where we're going.

So at a high level, there's five kind of tiers within the payment card industry field that people have.

About four or five years ago or so, each of the card brands, Visa, American Express, MasterCard, they all have their own operating regs, so you can go to visa.com, you can pull up their Visa operating
regulations, or MasterCard, and they are still required
to enforce those. The problem is, those regulations
were enforced to the banks, and the banks enforced that
to the merchants, and the merchants were saying, hey, I
can't support three different ways. Visa does things
differently than American Express than at MasterCard.

So what they did is, they kind of spun off a
separate entity, and so there's an entity called the PCI
Security Standards Council, and they're an independent
organization, and all they do is they publish documents
and set standards. So PCI doesn't fine anyone. They
don't go in and enforce anything. All they do is
basically publish documents. And if you go to
pcisecuritystandards.org, you can read about kind of
their programs and what they do.

Below them are the card brands. So all the
card brands have their own programs, but they also all
require all their member banks to enforce the
requirements in PCI. So they have something called data
security standard. They have something called the
payment application data security standard, which deals
with software and shopping carts which accept
information. And they also have the PED program, which
is the PIN encryption device program. So these new
programs are accepted and enforced with Visa,
MasterCard, American Express, JCB.

Below them are the banks. So if a bank wants to go and connect to VisaNet or ProcessAmEx, these banks at Wells Fargo will work with Visa and MasterCard to get that stuff up. The banks will issue those cards down to the merchants -- or to the consumer, as myself, and they'll also go and set up merchant IDs.

So it's interesting, because now you have two different areas. As a consumer, I'm worried about the protection of my card, and that's what my bank cares about. But as a member -- or a merchant, the merchant is concerned with their relationship with their bank. So when I go and I go to Wells Fargo -- or we'll use the table here. I go to Tully's, I pay with my Chase card, and they process through Tully's, and if Tully's is a Wells Fargo account, it's going to go up through there. So Wells Fargo would be Tully's acquiring bank, and then my Chase would be my issuing bank.

So it's important to understand, because different banks have different regulations, and because of that, what they're interested in is passing down that liability.

So what the banks have done is, now they enforce those requirements on the merchants. So there's about 1200 level one merchants out there, and these are
the largest merchants in the U.S., so they're merchants
that do more than 12 million transactions. And so the
payment card industry doesn't care about the value of
the transactions, because what they're interested in is
protecting card holder data.

And so whether I do a one-cent transaction or
a $10 million transaction, that card number is what's
important, because that's what can get stolen and what
can get used.

So it's important to kind of understand those
areas, because the compliance aspect drives from that.
And what you see is, basically, kind of, it rolls
downhill. And earlier, Jean Ann kind of asked and a
couple people have said, who really pays for these
compliance initiatives?

So just as with Gramm-Leach-Bliley and HIPAA
and all these other ones, when these laws get passed and
entities have to comply, the money's got to come from
somewhere. Most of them don't make less profits because
the new compliance came out; they find a way to kind of
spread that throughout other areas. And this is the
same thing for the payment card industry. So you see,
when there's a breach -- Hannaford's, for example, is a
good one that happened recently.

Hannaford's is a large grocery chain in the
northeast and they had a security breach. So what happens is, those credit cards that were divulged, their acquiring bank or their bank would have to go ahead and pay for those transactions. And what they're going to do is, that bank is then going to sue to try to recover those transactions from the merchant, and the merchant is then going to sue their assessor, like me, because they just -- it wasn't us, but someone like us goes in and says, in my opinion, you are compliant as of this date.

So realize, there's a bunch of different things that are in place, and it's just a way to make sure is that any issues that happen get passed down through Visa, through the banks, and ultimately to the merchants, and merchants end up working with the consumers, they have to forecast some of these things in their lawsuits, and they eventually have to kind of feed those costs back in.

So ultimately, the cost of compliance comes back to the end user. In my opinion, it's definitely a best thing. Just with Gramm-Leach-Bliley and HIPAA and all that, unless entities are required to do it, they're not going to go through and protect this.

The important thing is, there's only three programs that are being certified now, so when you say
that people are claiming to be PCI compliant or they're claiming something, right now, and I've worked with a lot of these different merchants, point-of-sale systems are not really deemed as PCI compliant right now.

When we look at things like ViVOtech and we look at these other areas, they're hardware devices right now and they don't fall under kind of the three general categories, and the three general categories are the data security standard, which applies to merchants that store, process, or transmit card holder data; they also apply to service providers that provide a service, like a payment gateway like PayPal; and then PIN encryption devices, so ones that are accepting PIN pads, those are assessed; and then applications.

So unless it's an application, a merchant, or a PIN encryption device, it's not falling under these compliance programs, and that's why there's some kind of uniqueness in the contactless field, because it really isn't governed. And the drivers from these are driven by Visa and MasterCard or the banks, and they all have their different types of -- and you've seen here, they all have different reasons of why they want to get that done, but in the end it's the consumer that has to pay for it and has to wonder, is that what you want to do?

So if Tully's would have to increase their
coffee by three cents in order to pay for the cost of
their compliance programs and assessment, is that what
you as a consumer want in the end?

And it's interesting, because as I do this,
the consumers are really driving this. So when Visa and
MasterCard and American Express first started publishing
these requirements, people didn't comply with them. And
now we see there is a general awareness now with folks
of, are they PCI compliant, about not working with an
organization that isn't compliant, and you'll see these
kind of disclaimers on people's Web sites or shopping
carts, so there is that, but ultimately the consumer is
the one that drives that. And if you don't want to be
using contactless or if you don't want to be using ones,
then you shouldn't be giving your money to those
entities, because they're going to drive those programs.

So let's talk about the threats that we have
now. So the threats with contactless, and we've gone
through a couple different ones here, if you look at the
statistics, in 2002, there's about 4,960 published
incidents of identity theft or accounts that were
compromised, and this was largely because there wasn't
disclosure laws in place. In 2005, that was 6.4 million
accounts. And last year, the estimates were about 162
million accounts. So chances are, half of us have had
something stolen. I've had mine stolen three times in
the last couple years. Once with the VA, with some of
that.

So, you know, it's interesting to see, this
is becoming a rampant field, and so folks in the
security industry are becoming well sought after, as
well as folks in the legal industry, because folks that
can wrap their arms around the technology, understand
the players, and then understand what really that
liability is and whether someone, you know, a reasonable
person took action that was applicable to this instance
is kind of an emerging area.

And that's where Hannaford's is interesting,
because as they got breached and the liability got
passed down to them, you see that they're going and
they're reaching out to Symantec, because they bought
Symantec tools that were supposed to keep them from
antivirus, they're going to reach out to their assessor,
they're going to talk to their bank saying, well, we did
what you guys asked us to, which is minimum compliance.
So it's really an emerging field out there.

For contactless, though, the market really
isn't that large yet from the hacker community. I mean,
it's great that we can run these, but right now, as I
said, there's two things: If you can steal the data,
and then what can you do with it.

Right now, the type of information profile, you know, names are not really considered areas, things that you can sell. But things like PAN, which is a 16-digit number, Social Security numbers, driver's licenses, those kind of go in the black market for between ten and two hundred dollars or so an account, depending on what you get.

So as we see those things kind of emerge, what the hackers really want right now from a credit card perspective is, they want to get the 16-digit number, they want to get the expiration date, and they want to get that PIN value, or the CVV2 or the magstripe. If they can create that, what they want to do is be able to create fraudulent cards.

The good thing with the technology, with RFID, if it's appropriately implemented, is that it would not allow them to do that. Because if they're not able to get that full information, they're unable to create a new card.

The problem that we're stuck with right now is that we have backwards compatibility. So when we look at our credit cards right now, you have the technology from 1950s, which is the embossed number; you have the magstripe, which then was the next evolution;
you've got the CVV number, which is the next evolution; and now you've got the contactless. So we've got four different levels of technology that we're carrying around and we haven't been able to retire those other ones. As long as we have those other ones, it's going to cause an issue.

So for CVV or the contactless right now, if it was fully implemented correctly and everything was encrypted and the CVC3 number was dynamic, there would be no way to take that 16-digit number and that card expiration and get a fraudulent account. Problem is, with backwards compatibility now, is that Web sites will take that, offline processes will still allow that to happen.

So until there's a way to address some of the retirement of the older compatibility, the newer security areas may still cause issues. And we just see that generally with PCs and computers. The more backwards compatibility you have with older systems, because they're legacy systems, you have to lower your security.

When we look at kind of the U.S. in general, there's about, I think estimates are about 400,000 payment readers, which is ten times more than anywhere else in the world. So obviously we're big consumers,
and I can't remember exactly where I was looking at it right now, but I think the average consumer has about seven or eight credit cards, and then I think the next country, I think is Brazil, which has one for every two folks. So it definitely is interesting to kind of see, as we get these cards and we're going to use them, what we're going to do as consumers.

The other thing is fraud detection. So we're worried about fraud and identity theft.

So there's two things really for identity theft. I'm comfortable using my credit card because if it's used, I don't pay the cost out of my pocket right now, and quite frankly, when I hand my card to someone, they can kind of take everything that's on there, anyways, right now. The important thing is the things like the Social Security numbers or other areas where you can't change those; those are the areas which are not now embedded in some of the RFID on some of the credit cards, and that is some of the things that helps protect us as consumers.

It's important to know because there's about 43 states now that passed identity theft laws, and those laws define what sensitive information is or define what personal information is very differently. So California and Washington define them differently; Alaska is
passing one here shortly. So it's important to know that, because when we talk about identity theft and what we don't want disclosed, we have to know what that is, because what you may see on a transaction, if it's a masked number or if it's just your, you know, a Wells Fargo account, it may not be considered sensitive information; you may not be protected under state laws.

So last, I just kind of want to say, there are different mechanisms out there. If you look over in Europe, they've got the EMV, which is a Europay-MasterCard-Visa system. So we see that there are different ways that people are doing this with the adoption. Here in the U.S., it seems to be the trend it's going to be towards this contactless information. In my opinion, just as with everything else, if it's designed correctly and implemented correctly, it will work.

The problem again is the backwards compatibility, and is it really designed correctly? And part of an assessor, we go and look, for an example, we see that credit card data is encrypted and we go and look and we see that it's encrypted, and we ask where the encryption key is, and the encryption key is stored in the same database that the keys are, so that's something of what the people that are designing the
systems and how they're going to enforce it are going to do.

As an assessor, all we do is we go in, and in our opinion, we go and benchmark them to the 235 controls or to some of the areas and we say, yes, these meet these requirements, or they don't.

So that's kind of at a high level how these things integrate. And if you guys have any questions, feel free to talk to me afterwards.

MS. MAYER: And I have one question.

MR. MCANDREW: Sure.

MS. MAYER: You just mentioned some state laws, and I'm not super familiar with it, but I know Washington state has a new law that became effectively, really, recently, specifically applied to the skimming of data on RFID enhanced identity cards, I think is how it's defined, and I think it was targeted at our enhanced driver's licenses and passports, but I'm just curious if that would apply to contactless credit cards or debit cards, as well.

MR. MCANDREW: I'm not an attorney, so there's probably a lot of attorneys can give that out there. But I can tell you, what's interesting is, as consumers, we were fed up with having our credit cards stolen, and there's no federal kind of requirement, so
we've pushed those up, and the states have required each
one, and each one is different with the limitations on
it.

What's interesting with some of these laws is
the extent that people do know how they can be enforced
or how they can't be enforced. Like, with the
contactless right now, I think the main driver, I
believe, is for passports and then also for driver's
licenses, because if you get a passport now, they're
issued with RFID chips, and if you're not comfortable
with that, you can obviously throw them in the microwave
or something like that.

DR. FU: I would not recommend that. That's
government property.

MR. MCANDREW: It's something to keep in
mind. Because from a security perspective, and you've
seen folks that can go out there, the limitation of the
two inches is because of the type of hardware they're
using in the connections, and the big concern out there
is that, I'm a U.S. citizen, I'm walking in a foreign
country, now people can go and detect me out there. So
there's a lot of folks that have gone through these
studies and said, look, we have that, I don't have the
option right now of not putting that RFID chip in my
passport, and I'm worried about kind of my security.
So there's definitely spectrums of what's operationally easier and then also what's operationally secure, and we've always got to try to find that happy medium in between.

MS. MAYER: Thank you. And there might be some more comments from the audience after we hear from our last speaker, who is Etona Ueda, who joins us from Japan's Nomura Research Institute, known as NRI, which is a major player in the communications and technology field in Japan. And Mr. Ueda specifically works on financial business consulting, and he's an expert in the market for and regulation of payment cards, and I think we're going to hear about how different the market is for the kinds of cards we're talking about in Japan. So without further adieu.

MR. UEDA: Thank you, Julie. I'm Etona Ueda. I'm delighted to have this opportunity to present Japan as a case study of e-Money. I would like to cover three main areas of e-Money in Japan.

So, firstly, I will give you an overview, and secondly, I will explain why e-Money in Japan, how rapidly it's become widespread, and finally I will mention some legal issues.

Overview. And today, there are 87 million e-Money cards integrating mobile phones in circulation.
There are several major e-Money brands and card issuers. Bordered in blue, you can see the number of users. And Edy, which is highlighted, is our biggest brand. But in terms of payment amount, bordered in red, Nanaco is number one. So therefore, there is no dominant player yet. And also, our company conducted a survey in four major cities. Close to half of the people surveyed said that they hold e-Money cards. But they did only major cities where an e-Money terminal is located in many stores.

There are two types of electronic payment services. The left side is the prepaid type and the right side is the credit card. Of course, I know that Visa and MasterCard offer a debit card, but debit card is very, very minority in Japan.

And railway operators and retailers have led the pack as major e-Money issuers, because they are a merit for both consumers and businesses. I will explain the detail in the next page.

And although postpaid services from credit card companies have made big efforts to promote their postpaid cards, but the total number of users is one seventh of that of prepaid cards.

The most important factor of the wider-spread e-Money is the core business function bundle, because
e-Money is mainly used for small payment amounts, as indicated on the left side of the table, and the income to issuer is limited.

Our survey shows that the average amount spent by use was about 600 yen, which means six dollars. In addition, operational costs are huge. The first session, the cost is limited, but there are so many costs, of course, terminal costs and network costs and the call center costs, so the costs are huge. Meaning, the issuer loses money on e-Money service itself, but they can make greater gains and reduce costs in some areas in their businesses.

Even with large operational costs and the fewer direct gains from providing the services, they are offset by the reduced cost of some operational areas, and I want to list advantages here. But please note, all listed advantages are not related to financial services. With these benefits and overall savings to business and greater convenience to users, this is the major reason why strict control by financial institutions as the only issuers shouldn't be enforced.

We estimated that the total amount of electronic payment in 2007 was about $85 million, and 75 percent of it was by e-Money payment. Based on the current growth potential, we estimated that the total
amount of electronic payment will be over $300 million in 2012, and that of e-Money will be over $200 million.

In this slide, I will briefly explain the technical futures of the contactless payment system in Japan. It is often said that Japan is a market in isolation, so the contactless payment system in Japan is also unique.

The total line in the table shows a kind of IC chips. All those services, including both prepaid and postpaid, use credit card chips with the Sony product and brand name, while the different standard worldwide is ISO standard. Because ISO14443 detects only IC chips, businesses have made efforts to adopt different standard in each area, such as OS application mobile. As Tom mentioned, Visa and MasterCard including JCB and (inaudible) are EMV contactless now, but all services in Japan do not use EMV contactless, even ISO standard.

In contrast to this, the physical system detects not only IC chip but includes encryption OS application standards. And it means that the (inaudible) optimizes (inaudible) security. So this is a reason why many businesses can launch their own services easily and their services are secure enough.
Transaction data is encrypted with one-time Password. It is similar to Visa and MasterCard. And the key is the different in each application, of course.

The next issue. This slide is current legislation framework. It shows what I believe to be the three reasons for the laws. One is to control financial businesses. The second is to protect consumers' money. And last is to protect personal data.

Looking at the first reason, should payment services be provided by a financial institution? Now, there is no existing legal framework, and FSA in Japan, I'm going to define what is payment services and who can provide it and how they should do it.

For certain reasons, we have all that law which focuses on prepaid cards. This law treats e-Money the same as prepaid cards and to protect consumers' money from the risk of business bankruptcy. However, the law cannot cover some kinds of e-Money, and it should be updated or rewritten.

The last reason shows general law. It protects personal data based on OECD's principles. And this provides more than enough protection for personal data. We have not had e-Money payment data that was stolen or used illegally in Japan. Personal information
such as name and telephone number is not necessary for analyzing and for basic marketing.

Most of e-Money issuers do not require consumers to register their personal data. On the other hand, detailed information is needed for exchange to CRM like one-to-one banking, of course. Therefore, consumers can choose whether they allow their data to be used and take benefits like point programs, or they do not allow much data to be used and they receive little, all based on the trustworthiness of each business. And this trust relates to loyalty, and therefore, people can choose which loyalty program may give them the best benefits.

The banking law designates deposit law and exchange transaction as business of banks. However, the concept of exchange is not defined in banking law, nor is it clearly defined by precedent. It is, therefore, unclear to what extent payments are included in exchange.

Because it is said that the payments are discharging of monetary liability, the FSA Japan seems to believe that the payment resembles exchange, but I don't think so.

The FSA is continuing to investigate the registration for the various payment services, and
debate over the scope of coverage continues. There are three main positions on this issue.

The first position or stronger view is that payment services should be included as exchange, meaning there is no separate payment category. And this would then require a new set of laws to be written for exchange services only. That includes control of payment businesses as the banks.

The second position or intermediate view, in the middle, that new laws should be enacted that covers only payment services but not exchange services.

The third position or weak view is that current regulations should be revised to address only the issue of e-Money. FSA seems to support the strong view, but I believe it is too strong for existing service businesses to adopt such regulations the same as banks, because they are not financial institutions.

I tend to support the more intermediate view. While I do agree stronger regulations are necessary to protect consumers, as I mentioned, the strong view is too strict.

And this is the final slide. In this last slide, I briefly look at the legal protection against the business bankruptcies. This law, called the prepaid card law, in short, treats e-Money recorded on a medium,
includes the card and mobile phones as prepaid cards. Because a number of businesses can issue prepaid cards, including e-Money in Japan, this legal framework is needed to protect consumers from the risk of bankruptcies of the issuer.

Major issuers need to resist government, and half of any unused amount of medium must be deposited by the issuer into a designated account at the end of each financial period. The account can be used in case a company goes bankrupt, ensuring protection of consumer monies. However, e-Money (inaudible) stored on a server, without physical medium, is not covered by this law. Because this law is too old, about '70s or so, so it did not foresee payment made as a result of any medium. This is the reasons laws should be updated, as I mentioned before.

Thank you very much for your time.

MS. MAYER: Thank you. I wanted to ask you one follow-up question regarding the fact that it sounds like many e-Money transactions can be anonymous, because consumers have the choice whether to provide personal information when they purchase a card?

MR. UEDA: Yes. Here is my transit card, and on the back this card, there is a blank for signature,
but I didn't -- and also a railway company does not know of who am I, only they know the ID, but they can understand when I use it and from where to where, and they can analyze what kind of doing I do, but they do not know who am I. And they don't want to understand who am I, so they don't request me to register my name.

MS. MAYER: Well, thanks for clarifying. I think a previous panelist had asked about that possibility with the cards we're discussing today.

I'd like to turn it over to folks in the audience. I think there will be some questions.

MR. MACCARTHY: We're all hiding in the back so we can throw spitballs at the speakers.

This is a great panel, and in many ways I wish we'd been on the same panel so we could have had a spirited discussion, but I think we might continue it during lunch, as well. But let me respond to a couple of things that have been mentioned.

First, the question, some people don't know whether the contactless feature is on the card and the sort of related issue of, I wanted to get one that didn't have the contactless feature and they sent me one that had it again.

Peter can speak to this, too, but there's no reason issuers want to hide this. I mean, it's not as
though people can use it without knowing they're using it, right? So every incentive the industry has is to make sure that people know they've got this feature on the card so they can go out and use it.

Now, there may be some failings in particular cases, you know, people don't look at the details on the card and they don't look at the symbol that's on the card, right? They don't look at the PayPass or the ExpressPay or the symbol that we've got, the indicator that has got the wavy lines on it, so they don't notice it's got the feature. That's a flaw in the communications system between Visa, the issuing bank, and the card holder. We really want them to know that.

The second thing, anybody who doesn't want one of these things for whatever reason, they've got a right to get a card that satisfies their needs and interests. If they don't want the card, they should be able to go to the issuer and get one that doesn't have the feature. If it gets sent back again with the same thing, again that should be something that in conversations with the issuer should be able to be cleared up. We don't want to create a situation where we're sort of forcing consumers to accept cards with features that they don't want.

On the incentives, the assertion was made the
incentives are all wrong. One of the things I took extra time in my time to sort of sketch out was that the incentives are right. The card holders are largely protected from fraud of unauthorized use of the cards right now. The people who bear the costs are the issuing banks. If something goes wrong, they have to pay the fraud cost. We think we've done a pretty good job. On fraud, our fraud rates are five cents for every hundred bucks. We have find no additional fraud associated with the contactless world.

Now, we monitor it, we can detect it, because we've got all those millions of cards out there. We put them on watch lists. We see if there's any additional fraud associated with that group of cards. If it's above five cents for every hundred dollars' worth of transactions, we know there's something that might indicate there's a contactless problem there. We haven't seen any of it.

PCI and encryption, that's a very interesting issue. PCI seems to be an issue with the merchant community at this point, because, you know, while financial institutions have been under an obligation to keep information safe and secure for a long time, it's just sort of getting to the merchant community and a lot of them are not completely convinced it's really their
responsibility. But I think we're moving ahead in that area.

On encryption, if there were a problem between general industry security standards and encryption of account numbers on cards, this has been a problem for a long time. Look at the front of your card. It's got the account number and the expiration date right there for anybody to look at. It's not encrypted. It's right there to look at. It's embossed on the card. It's on the magnetic stripe, as well. It's the kind of thing that can be read, not without some difficulty, but it is possible to swipe a card and read it and get the information from the magnetic stripe. So there's no general requirement that information on cards be encrypted.

DR. FU: I think I should answer that before you -- we'll have a good discussion over lunch.

MS. MAYER: Just in the spirit of making it a question, I just wanted to give --

DR. FU: I think the question is, is it the same as having it embossed on the card. And the big difference, there's a good analogy, and that is, with a contactless card, it's as if you've tattooed onto your forehead your credit card number and expiration date, and the question is, can it be read?
Maybe if you're, you know, on the other side of campus it cannot be read, but what if you're across the room, can it be read? Well, we don't know. What if the person has some kind of device that can extend the read range? Well, we don't know.

What we do know is that, well, if you're within a few inches you can definitely read it. But what we don't know is what's the physical limitations of how far away it can be read.

MR. MACCARTHY: And we can get into that at lunch, but let me just -- the second point associated with it, we've talked before, I think Susan had a question in the initial discussion, about whether the account number and the expiration date were in the clear, and the answer is yes. I mean, we're not disputing that. They're in the clear. If someone could find a way of reading it, they would be able to have that information. The question isn't so much is it accessible; it's what can you do with it once you've got it.

And the answer is, you can go to a situation where a card doesn't need to be present and you can try to commit fraud, and we have issues with resolving fraud in that kind of context; we're working on it. It's not the kind of thing where you're going to fix the "card
not present" fraud problem by doing something in the contactless space. It's a much bigger problem. When you solve the "card not present" fraud problem, we'll be able to address the contactless problem in a different way.

One last thing --

MS. MAYER: I just want to say, we only have about 15 more minutes for questions.

MR. MACCARTHY: I know, but that's why we should have been on the panel for this one, and that's why I'm taking this time.

DR. FU: Let's have dinner, too.

MR. MACCARTHY: That will be fine.

The final point about merchants sort of bearing the security costs here, there are no additional costs that merchants have to bear in order to do good security. Merchants do what they need to do to comply with PCI, and if they've done that, and if for some reason there's fraud associated with a contactless card, that wasn't their issue. They did what they needed to do in order to comply with PCI; they're fine. The fraud has to be paid for; it's paid for by the issuing bank, not by the merchant.

Now, merchants don't like to take full responsibility at this point for doing good security.
They've got issues with PCI, and some of those costs might ultimately have to be passed on to consumers as they do more and more security to protect information at their own premises --

MS. MAYER: Okay, Mark --

MR. MACCARTHY: But there's nothing on the contactless side that creates an additional problem for merchants at the point of sale.

DR. FU: Of course not.

MS. MAYER: And if you want to respond, but, Samantha, I'm going to ask if you -- I know, Jodi, you want to say something, but there's some folks over here who -- I just want to give the room a chance.

MS. GOLINSKY: And I'm sorry, sitting right next to the doctor, the person who talked about PCI, I have a question for you.

Financial institutions have had to safeguard customer data. One of the points you made was that you think that PCI compliance is being pushed down to merchants who have to pay for it and then they're ultimately charging consumers for it, so consumers are paying for PCI compliance.

Now, financial institutions have had to safeguard data under Gramm-Leach-Bliley Act for many years, and one of the things that I've actually said in
other panels that I've spoken on with FTC representatives is that we would love to see a uniform industry standard that applies to everybody in, you know, not just banks, but everyone in the industry that says you have to safeguard customer data. Is that something that you would be supportive of it?

MR. MCANDREW: Sure, I --

MS. GOLINSKY: The FTC doesn't have the authority to -- you know, GLB only applies to financial institutions. We have to safeguard customer data, our banks have to. Merchants don't have to under federal law; we'd love to see it if they did.

MR. MCANDREW: Sure, and definitely speaking as an assessor and as a consumer, we'd like to have that. The data security standard is, and I do a lot of governance work, is the most granular level -- there is no other standard I know that says you have to document all rules other than, you know, port 80 and port 443, it has to be signed by an officer. SOCS doesn't get in that level. HIPAA doesn't. So all the other regulations are built off of very general best practices.

So I definitely commend the institutions and the card brands for pushing this out there, but the problem is that the end merchants, like you say, if you
don't believe that the merchant pays for it, try working with a bunch of different merchants, because they're hiring folks like us to try to deal with this.

MS. GOLINSKY: (Inaudible.)

MR. MCANDREW: Sure, and I agree. I mean, as I said, we all want all of our entities to be secure, and in the past we haven't, and until recently, if we go to -- if you have a chance at two stores and one store has spent money on security and one hasn't and they're both selling hamburgers and one is an extra 50 cents, as consumers, we don't really care about -- we haven't, until recently, cared about security as much. Now, it's becoming security, and we see these companies are using it as a business driver. So because of that, that has changed a lot of the dynamics, and now companies are willing to invest because they see those returns on security.

MS. MAYER: And I'm just going to add quickly, that we are going to hear more about this at the end of the day in talking specifically about what the FTC has done in the area of data security beyond just financial institutions under Section 5 of the FTC Act, which is a more general statute.

AUDIENCE MEMBER: I'll make my comments quick here. I think it's clever that there's foil on new
cards as they're traveling through the mail; that's the first time I've seen that.

Regarding the issue of consumers having a choice, the local bank actually issues only PayPass-enabled cards. You don't actually have any choice in the matter.

As far as encryption, there basically isn't any, so these statements and PR releases are actually patently false, as far as I can tell, from the RF perspective.

On the topic of detecting fraud, many current integrations that are done at point of sale are actually emulating additional magstripe data, so it's using very traditional systems, integrating bolting onto existing point-of-sale systems, it makes integration very cheap, right, they don't have to change anything, there's no back-and-forth communication with servers. So the net effect on that is, it's very hard for most issuers and banks and processors to actually detect fraud, because they can't actually tell the difference between a contactless fraudulent payment and a magstripe one.

I think as these new security features get deployed, that will become easier, but most cards have the exact same information on them. American Express uses different credit card numbers encoded on the RFID
than on the magstripe, allowing them to do much more advanced and sophisticated detection.

I think this entire topic of security is not very well understood by consumers and issuers and banks, and there's a lot of hand-waving, "Oh, it is secure," when in reality there's a whole lot of unknowns, and a lot of hand-waving that's occurring.

So in my mind, if we're going to move forward with the wireless payment system, it should use real crypto and have public peer review from industry people that know what they're doing as far as security, and that hasn't happened today.

Thank you.

MR. HO: Can I comment on that, real quickly?

At the end of the day, there is a way for us to identify contactless transaction, and so we can tell whether or not it is by magstripe or by contactless. So I think the thing here is, and I welcome the open dialogue, but many assumptions are being drawn about technology that I would welcome -- like I said, I would welcome the dialogue, but before we draw to conclusions of what is and isn't real, let's make sure we have all the facts.

AUDIENCE MEMBER: So the current readers emulate the magstripe technology?
MR. HO: That is correct. So the readers, basically, it's magstripe data that's being transmitted. However, there is a specific transaction code that every acquirer must carry as a part of the mandates from the association so that we can identify them.

AUDIENCE MEMBER: (Inaudible.)

MS. MAYER: Can we just wait for the mic, and I think -- Eileen, do you want to -- and then we'll get to you.

MS. HARRINGTON: A couple of the panelists raised the risk of identity theft in connection with RFID-enabled, contactless-enabled cards. The professor from U-Mass showed that video that raised the question of identity theft, and then, Tom, you mentioned it, although the numbers that you cited are, I think, numbers that are associated with account information breach, not actual creation of new accounts, and the kind of identity theft that we think of as being harmful to consumers.

I'm wondering, Peter, number one, whether the scenario that was displayed in the video is one that you think can be replicated; that is, is it possible for a nefarious being to come up to folks with a reader and lift this kind of personally identifiable information from cards? That's a yes or no question. Is that
doable?

MR. HO: It is doable.

MS. HARRINGTON: Okay. And then my next question is, what we know about incidents of identity theft that are associated with stealing information this way, from contactless, from devices that are enabled for contactless payment; does anybody have any data on that?

MS. MAYER: Why don't we give Jodi --

MS. HARRINGTON: Well, actually, anybody on the panel, first, have anything on that?

MR. MCANDREW: I can just tell you from an incident response perspective. What the card brands are worried about and issuing banks are worried about are large data stores, so they're worried about multi-thousand dollars of data as it's stored in databases that are accessible. I mean, they definitely are concerned about individual one-offs, but I'm not aware of any large --

MS. HARRINGTON: Right, but from the consumer standpoint, the individual one-off is often the most dangerous situation in terms of identity theft that causes harm.

MR. MCANDREW: From my experience, no, because from an incident response perspective, there is no response to that. Resources are being spent in
those. It's easier just to reissue a card and take losses for a while.

MS. HARRINGTON: I have a follow-up question. Is there something that -- do you have very specific recommendations for what could be done with contactless-enabled devices to make them safe from the kind of skimming that you demonstrated?

DR. FU: There are some techniques that can be used. They do have costs. There are infrastructure costs, and it's obvious it that those are -- there is always a trade-off. Almost always, there is going to be a trade-off on how much it's going to cost to make it more secure.

MS. MAYER: And while Samantha is passing the mic, I was going to say, we are going to hear more about specific measures that are available from another doctor, Kohno, later today, on one of our panels.

MR. HO: Actually, Liane, before you speak, just to answer your question even more fully, Eileen: You know, regular men's wallet. I have my contactless card in here. (Demonstrating.) There it is.

But the reason why, first of all, contrary to popular belief, we're not transmitting data off the card. There is no power source on it. So it takes some time for you -- because the power is coming from the
reader, and so it took me that long to get a read, because you had to power up the card.

AUDIENCE MEMBER: So now that I have your card number and expiration, I can write that to a magstripe and conduct fraud with it?

MR. HO: No, you can't, because you don't have the CVV1 in front of you.

DR. FU: Do we have permission to use that information?

AUDIENCE MEMBER: You know, I'll give you a test card.

MR. MCANDREW: No, no, to that point it's very important to understand that the magnetic stripe, there's track one and track two data, and that information is different than the CVV number, which is on the front, which is different than the CVC3 number. So each one of those have different data and you can do different things with them. The issue is that if you still have the 16-digit number and expiration, under a lot of areas, you can still process.

MS. REDFORD: Tom, I just want to echo that. Earlier, it was stated and we want to make that very clear, that the contactless application has simply the same information as the magstripe. No, that's absolutely not true. There's information laid down on
the magstripe, and there is an encrypted value
associated with that that we've been using for a very
long time at Visa, very successfully, to counteract
counterfeit.

For the contactless data that's on the chip,
that data and the secret key on the card creates
information that is assembled by the merchant's point of
sale in the same format as the magnetic stripe, because
it flows on the same message format through the Visa
systems, but the data within the transaction is
different. That data includes that encrypted dynamic
value which is different. And it includes, as Peter was
pointing out, we have defined values that when Peter
gets the information at his system, he can tell, is this
a magnetic stripe transaction? Great. This is how I
validate the code. Is it a contactless transaction?
This is how I validate the code, or Visa will do that
for him.

So we can differentiate if data is being
lifted from one attribute of the card to another
attribute of the card to fight that counterfeiting and
skimming.

MS. MAYER: I think we have time for at least
one more question, and I think we'll all be going to
lunch.
MS. GRANT: I want to preface my question by saying that the consumer ends up paying, regardless. If there is fraud, and also for preventing fraud, and it doesn't really matter whether the merchant ends up being liable or the issuer, the consumer ultimately is the one who pays.

So one thing that is disturbing me is that we have these protections like the three-digit security code that can be used on the card to prevent somebody from taking that information once they've stolen it and giving it to everyone they know online and enabling people to make online or telephone purchases, but it's up to the merchant whether or not to require that information that supposedly protects people. It's not mandatory for them to do so.

So do we need mandatory requirements that are set by industry? Will that work? Or do we need laws that require that kind of mandatory adherence to practices and procedures that can give consumers that protection?

DR. FU: Can I adapt that? I'm curious, what kinds of security options did Visa provide Wells Fargo? What options were you allowed to choose from in implementing on your device, and how does the consumer know what choice you made?
MR. HO: At the time, we were given options. Back then it was known as best practice whether or not to name-mask, whether to shield the card. However, the dynamic CVV was a requirement for us to implement. There was no other way we can go to be certified. We were highly -- it was highly recommended that we shield both the name and in the mail stream, and we had extensive risk management conversation, and it made very good sense for us to do it, so we did.

I think at the end of the day, the industry has no incentive to have its name sullied, if you will. We're not incented by having our reputation dragged through the mud, right? We stand for something, and we trust that our customers trust us. And so when we measure and when we regulate ourselves, we regulate ourselves to the highest standard.

Now, I'll admit that there have been breaches and things that people -- we're human, we haven't all figured out everything, so we fix them as quickly as possible. Then there are also -- there will always be people who are motivated to take bigger risks than others, right? And that's where I think the associations like Visa and like MasterCard will prevail in terms of how they mandate the issuers in terms of how we protect the customer and how we protect the
technology.

    DR. FU: So there are many associations, many
different standards, and since you're one of the expert
consumers, I was wondering if you could tell me on these
cards, which ones protect the name?

    MR. HO: Those are not my cards, so I can't
speak to them.

    MS. MAYER: And I think, you know, we can
have discussions also after, but we're pretty much at
the end of our time here. And I just want to express my
appreciation for everyone on the panel, in particular,
and also being here to be as honest as possible with us,
and I appreciate that. The FTC appreciates that a lot.
    And for folks in the audience to making this a very much
true to the town hall spirit and being active
participants, which is what we really want.

    And I think we've laid out some challenges
that, I don't know if they'll be answered, but they'll
certainly be addressed in certainly our last panel of
the day, so I hope everyone is staying around, and the
panel preceding that will be very interesting, as well.
    Lunch, I guess which will also be very
interesting, if you would like to join us just for an
informal group lunch on campus at the dining hall at
Eight and McMahon, and Charles over here will be -- if
you want to follow Charles with just the group on the
tour to get there, it's about a ten-minute walk.

Thank you.

(Recess taken.)
MOBILE PAYMENT DEVICES

MS. RATTE: Okay. I think we're going to get started now, everybody. Thanks for returning from lunch. I know it was tempting to stay outside for a little while.

With this panel, we're planning to turn our attention a little bit to the future. We've heard a little this morning about mobile payment devices, cell phones, and in this panel we're going to explore where that technology is, where it is in different markets, in fact, both in the U.S. and abroad, and whether there are any consumer concerns specific to this type of technology, how consumers are reacting to it, how they understand it.

So we're going to get started with Dax Hansen from Perkins Coie, who's here representing CTIA, the wireless association, and he'll layout some of the business case for mobile payment systems.

MR. HANSEN: Thank you, Katie.

These are very interesting times, and we can all see that the nature of money is truly changing, and the mobile device and wireless are driving many of these changes.

The mobile makes contactless payments more than a swipe replacement. It makes the payment
experience intelligent, engaging, relevant, and trusted. It offers security features and technical capabilities that can improve the user experience, can authenticate users and payment transactions, and can mitigate fraud. And although there are many benefits that wireless and mobile bring to contactless payments, a few of which I've put on this chart, I'd like to just highlight three.

First, the ability to know the customer and where that customer is located. Second, reliable and secure networks. And third, robust user interfaces. Authentication is a term of art that we're very familiar with in the payments industry. What it really means is that you can determine that an individual is authorized to make a certain transaction. Authentication is required by most of the payments laws, certainly by the payment association rules, and it assists with fraud mitigation, consumer protection, customer care, and other aspects.

And wireless carriers know their customers. Mobile devices are associated with a wireless account, with a telephone number, and other device identifiers. And this ability can be leveraged to authenticate mobile payment transactions and to offer other benefits and opportunities that have not traditionally been available.
in payments.

Wireless protocols such as GSM and CDMA include baked-in security features, such as spreading sequences and shared keys, that arguably make them more secure than the Internet, over which many of us conduct payment transactions today. And the handsets and the mobile wallets that are being loaded onto them support encryption, PINs, and other security and access control features that have not been traditionally available.

In addition, wireless carriers currently maintain over-the-air provisioning capabilities and infrastructure that may be leveraged to provision some of the payment cards to handsets and to manage the life cycle of those cards in ways that may be more secure than current processes.

Just a note here, it's been very clear through the morning session that we understand that RFID technology uses a communication protocol that does not rely on the wireless carrier's network. That's independent. So in addition to the security features that we've already heard today that just exist with RFID, you can layer on top of that certain of the security features baked into wireless networks to the extent the payment system really needs to touch that wireless network. And it may not, in too many ways, and
certainly not for the point-of-sale transaction where it's really being read from a reader and the handset, or from one handset to another handset.

Perhaps the most exciting feature of mobile is that mobile devices have screens, and they have interactive applications on them that can make dumb payment cards smart. And suddenly, they offer consumers access to realtime purchase information, realtime transaction information, realtime balance inquiries, proof of purchase, mobile coupons, or other content or information that help inform and improve the purchase experience.

Consumer protection and regulatory topics arise in any payment environment. A CTIA mobile financial services action team has been evaluating privacy and security, disclosures, authorization, access controls, fraud prevention, protection of minors, dispute rights, and other topics, because it is appropriate to consider whether the mobile device and wireless create any new concerns and how the mobile impacts traditional concerns.

My opinion is that the mobile improves on the traditional concerns, in part because of the mobile facilitates better disclosures and transaction information, user and transaction authentication, access
controls and security features, and fraud mitigation, among other things.

This is an evolving industry. There are many open questions. Questions regarding openness: open networks, open platforms, open devices, open software applications. Questions about how to apply existing laws and regulations to emerging business models. There won't just be one business model for mobile payments. They'll be as diverse as the players who have been presenting today, and you have an interest in the financial services industry and in wireless and in Internet. The players here will be very diverse, and that will cause additional questions: Who are the players? How big is this value chain? How do we come up with business models that make everybody happy?

In the end, I think someone made a comment that a contactless solution doesn't have a value proposition in and of itself. It can be leveraged in new and exciting ways to create revenue opportunities and better customer service and consumer experience opportunities that consumers will demand, that they're already demanding. We have a very sophisticated consumer base.

Despite those open questions, I think it's clear that somebody will always be minding the store.
There will always be, just like in any traditional payment system, one or more program providers who are promoting and providing the payment service, the mobile payment service, to consumers. And those program providers will be responsible for consumer protection and compliance considerations.

So to recap, the mobile and the wireless industry bring to contactless payments capabilities that enliven contactless payments. Mobile payments certainly touch on consumer protection considerations but improve on those concerns and on the user experience. And because of the benefits that wireless and mobile can bring, the wireless industry is well suited to help the contactless payments industry develop.

Thank you.

MS. RATTE: Thank you, Dax. That was a great overview of the business case for this technology.

Before we turn to Susan and some of the consumer concerns, I just had one question for you. It seems to me that one of the big changes we're looking at here is around location tracking; that's really the big difference that this technology is bringing to the table. So has your group looked at disclosures specifically around location tracking and giving consumers choices about whether or not they want to be
1 tracked?

MR. HANSEN: Certainly. If you haven't seen
2 it yet, you might look at the CTIA's Web site for the
3 location based services best practices guidelines. The
4 wireless industry, as a whole, put a lot of time into
5 anticipating these questions that might arise in the
6 consumer protection context and laid out a very
7 thoughtful set of guidelines and best practices that do
8 revolve around the two main principles of consumer
9 notice and consumer consent.
10
11 And I guess it's fair noting here that the
12 wireless carriers don't want to create an unpleasant
13 user experience. They spent a lot of time trying make
14 sure that the consumer experience is helpful, is
15 streamlined, and the last thing they want is a bunch of
16 calls coming into their call center about one of these
17 particular concerns. So they do think about these
18 things and try to address them, so I'd recommend those
19 guidelines for review.
20
21 MS. RATTE: Okay. Now, we're going to hear
22 from Susan Grant, who's Director of Consumer Protection
23 for the Consumer Federation of America.
24
25 MS. GRANT: Thank you. I should start by
26 saying that contactless payment in general and mobile
27 contactless payment offers many potential benefits to
consumers. So we're excited by it. Clearly, mobile is the Holy Grail of contactless payment. All the forecasters say that this is what's going to drive widespread adoption of contactless payment by both consumers and merchants.

But mobile adds new dimensions to many of the concerns that we've spoken about this morning and raises some new concerns, as well. And I've done a slide that just lists many of the consumer concerns. It's not an exhaustive list, but probably the main ones that I want to cover.

We've talked about privacy already, and location information in particular is an added dimension when you think about mobile contactless payment, because you have the information in your mobile device about where you are. You also have other information that may be stored in your mobile device. And all that information, if it was possible to put it together and splice it and dice it in different ways, could provide even richer targeting and tracking of consumers for all sorts of purposes, marketing and otherwise, in what as has been mentioned earlier have previously been largely anonymous types of transactions.

And consumers' privacy is not really adequately protected by the legal regimes that we have
right now. We've got specific rules for telephone companies in terms of what they can do with customer information and how they can share it, and under what circumstances consumers can opt out or what circumstances require consumers to opt in for their information to be shared with others. But of course, the information doesn't need to be shared with others. It could be used by mobile carriers in revenue-sharing agreements with consumers to market them without ever having given consumers' location or other information to business partners.

Location and other kinds of information can also be collected in ways that are outside of the mobile carrier's purview. Location information can be captured by RFID regards at different points where consumers may pass through doorways and so on. Information can be captured by applications that are either put on consumers' handsets to begin with by the manufacturers or the retailers of those handsets, or downloaded by consumers at a later date that can provide location and other information.

So the one thing that is clear in this confusing situation is that the phone or the PDA is no longer a communications device. It's a device that has a wealth of information on it and that can be used for a
variety of purposes, and consumers may not be aware that
sensitive information that may be in it can be used and
obtained in different ways.

We've talked a lot about security today, so
I'm not really going to spend a lot of time talking
about that now, except to say that I'm not reassured by
what I heard this morning. In fact, I think I'm more
confused than ever.

And I'm not assuaged by the argument that
businesses will adequately secure consumers' information
because it's good for them to do that, because, of
course, it is good for them to do that, but when we see
just data breach after data breach and sloppy practices
and situations where it's clear that companies are not
putting the thought and the planning and the money into
the protection systems that they need, then I think that
that concern is even more heightened when you have a
device that, unlike a card that's in your pocket you're
carrying around with you, you put down somewhere where
someone else might be able to get it and take it and use
it, the device itself is not very secure and it's
ubiquitous and widely exposed.

It's great that the mobile providers can
provide things like PIN numbers and so on to give
consumers the protection that they need, but then my
question is, will that be the standard practice or a
required practice, or will it just be another best
practice that companies will adopt or not.

Jean Ann touched on dispute rights this
morning, and I'm not going to go into that in great
detail, either, except to say that we are still
concerned about the fact that if the billing is done to
the mobile service account or to some other kind of
account that is not clearly regulated as a financial
account, consumers don't have dispute rights and legal
protections, and those are clearly needed.

And also, if you are doing something with
your phone like buying a transit ticket or something
where you may need to show proof of purchase or get a
ticket for turnstile jumping, and all the sudden your
battery dies or for some reason your device doesn't work
or the program malfunctions, there is a concern about,
how do you show that you've actually made the payment
when you don't have something, a piece of paper that
proves that.

Children are a special concern, because while
children are not carrying credit cards and debit cards
around, they are carrying mobile devices around, and if
those devices are enabled to make contactless payments,
there need to be easy-to-use controls that should be on
by default and that shouldn't cost parents anything to
limit or restrict what their children can do. There are
cravings about over-consumption, not only by children
but by adults, and I think Jean touched on those this
morning, as well as things that people might do with
their devices that are things that by society we might
not want to have happen, like gambling using your mobile
device.

And the last thing that I want to talk about
which we haven't really talked about today but is very
important for consumer advocates to flag, is choice of
payment providers.

Right now, I have several different kinds of
cards in my wallet. I have airline cards, I have a
debit card, I've got cards that I use jointly with my
husband and then cards that only I use, and I have a
choice when I make a payment of which of those payment
mechanisms I want to use, and I decide on the basis of
many personal factors which one to use.

But we're concerned that there's the
potential for consumers to be told you can only use
certain payment systems with this particular device,
either because the device manufacturer or their mobile
service provider has some sort of exclusive arrangement
or because the device just isn't capable of running the
payment system that you want to use.

So just as in the broader argument over things like net neutrality, the payment system has to be an open system where consumers can use the types of payment mechanisms that they want.

Thank you.

MS. RATTE: Thank you, Susan. You've certainly given us a lot to think about.

I think we'll move on to the next presentation and save some of the questions for the end. So now we're going to hear from Peter Wakim, who's Director of Business Development and Strategy with Nokia.

MR. WAKIM: Thank you. I wasn't here this morning, but I heard that there was a lot of interesting discussion. I've been working on RFID and contactless technology since about 2001, and I've had a lot of experiences with consumers, running trials, getting their feedback, understanding their concerns.

So what I'm going to discuss with you today a little bit about -- I'm sure you've heard about NFC; I don't want to spend too much time on that. I want to look at some of the concerns and some of the safeguards that we have tried to apply to mobile in our thinking, and some feedback from a recent trial we've run on
contactless payment.

So NFC, as you have probably heard, is based on a short-range RFID technology, and not only does it enable what we've been talking about today, contactless payment, it also enables a very unique user experience. By actually using your mobile device, you could actually interact with the world.

And it's been designed around industry standards, and clearly the goal has been to have a very short reading range, so it's not a high power technology. The idea is that you would virtually have to make a decision that, I want to touch something with my phone.

Not only, as I said, have we looked at payments with this technology, and you've heard a little bit about ticketing as well, transit ticketing, but not only bringing two mobile phones together, I could share content. So if I explicitly wanted to pass a picture to you from my phone to another phone, this technology would enable that sharing of content.

It also would enable consumers to interact with, say, smart posters. If I wanted to find out more information about a particular item or a map, if that poster is what we call a smart poster, I would be able to touch that poster, maybe download some content or
interact with that poster to get more information. And of course, payment is another opportunity that consumers could potentially use this technology for.

Before I start talking about some of the concerns and safeguards, I'd just like to get a show of hands: How many of you have actually made a point-of-sale purchase with a mobile phone?

One, two, three, four. So actually not a lot of actual real world experiences. I've personally been involved in a number of these trials and carried the phone and know what the experience is like, and I want to actually run a little video just to give you the vision of what it really is like, because I think, unless you've seen it and done it yourself, you know, we're talking PowerPoints right now, so if you'll give me a second.

(The video was played.)

MR. WAKIM: Okay. So just to give you the flavor of what that's all about, and to also give you the flavor of where we are as an industry. We're not commercial. We have been running a lot of trials using potentially not even commercial phones. That phone you saw there was the first commercial phone capable of doing NFC transactions. So we're in a very early stage. And as I said, we've been working on this since 2001, so
we're not running as fast as you may think.

Now, some of the security issues. Of course, as I've said, I've interacted with hundreds of these users. I've been one myself. I'm a consumer. Of course, I have my own privacy and security concerns. And clearly the architecture needs to be as secure as possible.

And I know the standards are there. The credit card companies, the banks, CTIA, everybody is working together to try to pull together a very secure and standardized platform that would allow this to happen. And from Nokia's point of view, we are a consumer electronics company, security is extremely important for us as a company, and we do not want to proceed with a technology that we know is flawed or insecure.

I don't know how much has been addressed about the technology itself, but the contactless credit cards utilize a secure element, and inside the phone there is a secure element. It may reside in the phone, on the SIM card, or on a memory card. And this is a very secure protected area of memory that only the application for the payment and certain keys are held. And the credentials for the credit card are in the secure element.
So when you make that transaction, the key is never transmitted which produces the next CVC code. So even if you did have a rogue reader to pick up your credit card number and the CVC at that point, you could never do the next transaction. The CVC would not line up with the next CVC.

Going back to what we heard before about the added features of a mobile device versus a traditional contactless card, we have a complete user experience now. We have a keyboard; we have a display. And on the trials that I've been involved in, the last trial, for instance, the secure element had a PIN code enabled, so the contactless card itself was PIN-enabled. So the user, when they wanted to make a transaction, entered a PIN code to then set the transaction ahead, and then the credit card itself is not visible anymore. So it was only for that short few seconds that you made the transaction.

This could be taken further as technology evolves, where biometrics such as fingerprints could be used. So there's a lot of potential safeguards there. As I said, the CVC code is highly secured inside the secure element, and it is a dynamic code, unlike a magstripe where it's -- I just had lunch; I gave my credit card out to the waitress; she had my
whole name, card number, CVC, my signature, everything was given away.

The other thing, when you first give these people phones, a lot of these concerns raise up, but then when they start comparing to what they're doing now, putting their cards online, handing their cards around, then they start to realize actually they've got an added level of security here, and if they lose their phone, which most people would notice that much faster than they notice one credit card falling out of their wallet, it could be disabled over the air, which we don't have that capability with a traditional credit card. So, again, there is another level of security that mobile can bring.

And just to give you some feedback from that trial that I just showed you the video for, people are extremely excited. We actually were able to recall the phones and shut off the credit cards, but a lot of people wanted to keep the phone active. It was a trial. And really, the enthusiasm of the users was overwhelming from a convenience point of view, because most people carry their phone wherever they go. They have their keys, their phone, maybe their wallet, and sometimes people forget their wallet. More than likely, if you leave the house without your phone, you'll go back. And
more than likely, you'll notice your phone missing
before you notice a credit card missing from your
wallet.

So that's my presentation. Thank you.

MS. RATTE: Thank you very much. I just have
one very brief question while Siva is getting ready up
here. You mentioned that you're still in the trial
phase. Do you have any forecast of when this might be
available commercially in the United States?

MR. WAKIM: I think it's up to a number of
different parties. I mean, we are a mobile phone
manufacturer, and we're working with all the parties to
make the technology as secure as possible and to bring
it to commercial launch, but as you know, the credit
card, there's a credit card company, a bank, and in this
case the mobile operator is the distribution channel for
a mobile phone. A lot of those different ecosystems
have to be in the right balance before this can be
happen.

MS. RATTE: And are you seeing speedier to
market in other parts of the world?

MR. WAKIM: Yeah, I mean, clearly, Japan and
Korea have embraced the technology much faster.

MS. RATTE: And what about Europe?

MR. WAKIM: There's opportunities in Europe
around, especially there's a lot more transit, where
people use metros every day or buses where there's
contactless tickets, so that's really the front line,
where U.S., more than likely, payment seems to be the
driver here. No more credit cards or debit cards.

MS. RATTE: And we'll continue this
discussion with later speakers, as well.

Now I'd like to introduce Dr. Siva Narenda.
He actually said I could just call him Siva, but I
thought I'd attempt his last name. He's Co-founder and
Chief Technology Officer at Tyfone, and he's going to
talk a little bit more about the security features that
we've been hearing about.

DR. NARENDA: Thank you, Katie. Thanks to
FTC and University of Washington for putting this forum
together. It's been very educational, although I've
been doing this for the last four years. Thank you for
being here. It's a beautiful day outside. It's a shame
that you're sitting inside, because I'm from Portland,
and Portland and Seattle, usually summer falls on a
weekend, so we try to make the best of it.

I will be not talking really about security
or privacy, whether perceived security or real security.
I think there will be issues. We're all engineers at
heart, at least I am, and we'll figure out a way to
solve all those problems.

But what I'm here to talk about is to pick up on what Susan said at the very end of her presentation, is talk about a specific issue which is related to consumer freedom of choice. And I'll go through some historical examples and technology answers that have been present historically and then try to draw parallels the best we can into mobile contactless payments.

I want to differentiate Near Field Communication from mobile contactless payments, because Near Field Communication, as the gentleman from Nokia explained, is actually a super-set; it's got a lot of capabilities, including contactless payments.

So you and me and everybody as a consumer today do have a freedom of choice. We get to pick whatever phone we want, to a large extent, and pick any network operator that we want, and pick whatever card-issuing bank and checking account bank that we want. And that's really critical for all of us, and you will see some examples that actually go against it and it has not been successful.

So what happens in the way the contactless payment in the mobile world is architected changes the flow as follows, and this is to what Susan was talking about. And it's architected for a good reason, by the
way. This is not something that just fell out for no reason.

So what you basically have is network operators that work with device manufacturers to provide telephone services and data related services. All of us love it; we use it. Some of us have more than one phone. But the moment you bring mobile contactless payment, the logical way for it to fall out is exactly as shown about. The network operators have to sit in the middle, because they are the ones who own the security element, be it a SIM card or a secure element integrated in your phone. If you're using a GSM phone like AT&T or T-Mobile, you'll get one of these; if it's Sprint or Verizon, it's probably integrated inside the device, at this point, anyway.

They own the SIM, the secure element, because that's how they provide the service, and that's how they guarantee to provide service. So if NFC solution, the Near Field Communication solution integrated inside the phone needs to store account information securely in the same secure element, the operator has to be in the middle, because this is theirs, this is their technology, this is their security.

Therefore, financial institutions have to work with operators to enable mobile contactless
payments. There's nothing inherently wrong with that. It's theoretically very possible. Practically, it's got a lot of issues. I'll highlight one of them, and there are several.

In the United States, you have 10 major carriers and 180 in total, and there are 18,000 financial institutions. For this flow to work, you really need a matrix of business relationships that is impossible. And believe it, service managers aside, that just complicates the problem.

So, now, this is not the first time something like this has been attempted, so let's go back in history and see. Online banking and online payment architecture was precisely built exactly that way. Internet service providers, America Online, Prodigy, CompuServe -- this is a figure from a book that was written about the history of online banking and payments. (Inaudible) in the middle, because they were the consolidators of providing service. They were the content providers, and banking happened through them, and so did everything else.

But obviously, we know that this was not the model that prevailed. This is the early '90s. In fact, when I was trying to understand more about online banking, I actually discovered something that was even
older, another example that didn't work. I don't know how many of you have heard of Viewtron; I hadn't until the day before yesterday. This was actually a service provided in early '80s. It was in about 15 cities. It was actually started by AT&T, with a couple of newspaper companies, to provide content and services to customers. They spent about $15 million in 1980. If you're interested in Google or Microsoft, that's probably worth about five, six billion today. But nevertheless, it's a model that didn't work, for obvious reasons. Again, consumers don't have choice, what Susan pointed out.

So it's a difficult problem to solve. And generally, solutions have come about with an appropriate technology, and in the case of the two problems that were discussed, the appropriate solution was the Internet, and the Web browsers that made it more open. So today, Comcast doesn't tell me I have to bank with Citibank. So you have any computer, any ISP, any bank. This model prevails, and everybody makes their own money.

Now, how could something like that be possible in a mobile environment? It may or may not be possible. Here is one particular solution. This is something that we built, but I'll leave Tyfone aside.

Secure element can be a memory card. I don't
know if you've seen one of these. This goes inside your camera sometimes, or a lot of the phones have these these days. So this can be the secure element that your card-issuing bank or association issues to the consumer independent of this. Right?

It has a built-in antenna, so it doesn't really require the device to have the full NFC capability for payments. NFC has a far-reaching application set, lots and lots of applications, which has got nothing to do with payments. So this is not meant to be the NFF be-all, end-all contactless payment. Contactless technology is purely about payments and independence consumers need to the point that was raised a little bit earlier.

So it's interoperable. You can tomorrow decide to go from AT&T to Verizon, which doesn't have a SIM card. You can take a memory card and put it in the phone and continue your relationship with your card-issuing financial institution.

So now the question is, so where all can we use this?

This is data from April of this year. In the United States, 57 percent of the mobile phones have memory card slots, across all carriers. Globally, that's a monstrous 600 million phones. And memory card
slots generally were associated with smartphones. Four years ago when we started, there were two models available with memory card slots. Now, it's exponentially grown. It's available in a wide variety of devices. And NFC phones -- this does not compare the two. NFC has definitely a whole bunch of other applications that have customer convenience beyond payments.

So the point, therefore, is to retain freedom of choice for the customer, pick any phone, within codes, get a secure element from the operator to have a relationship as a consumer with the operator, and your card-issuing bank gives you this to have a relationship with the payment entity.

Will this model be successful? We don't know. This may take 20 years to be successful. If you remember, Viewtron started in 1980 and by the time Internet banking really happened, it was 2000, right? So it's not clear whether Tyfone will participate in it, and for that matter, for this discussion it really doesn't matter.

What's important is in the long-term, retaining freedom of choice for mobile contactless payments is extremely critical, and the financial institutions and carriers and payment associations have
to pay attention to this. I'm not sure how much
attention has been paid in the NFC forum. Up until, I
would say, middle of last year, memory card as a secure
element was still a discussion item. It was not really
committed. It has been at this point, so it is a viable
option. A technology has to be available, a viable
technology has to be available to provide this
independence, if you go back in history.

I'll stop with that.

MS. RATTE: Thank you very much. I just had
one quick follow-up question. Since you're talking
about consumer choices and benefits that this can
provide for consumers, have you given any thought to,
you know, in this pretty technical space, how to teach
consumers about how this whole process works? You know,
when you were talking about things that are highly
technical like this.

DR. NARENDA: That's a very good question,
actually. And that's really where the SIM cards have a
significant advantage, because a street vendor in the
corner of China knows what a SIM card is.
The only way that the alternate secure
elements will be educated to the consumers has to be
through financial institutions and stakeholders who have
potential value in it in spending a lot of marketing
dollars to educate the customers. It can't be a technology play. It really needs to be a use-case play, explaining to consumers what options they have and how they use it. There is no way around that; there is no shortcut.

MS. RATTE: And I wonder, Susan, do you have any reaction to the presentation on consumer choice? Does this address some of your concerns that you raised before?

MS. GRANT: Yes, it does, and I agree with your comments about education, as well.

DR. NARENDRA: Right. And because it's independent, you do have the choice to either have it or not have it inside your device.

MS. RATTE: Thank you. Now we're going to hear from Andras Vilmos, who is coming to us from Hungary, traveled a great distance and we thank him for that. He's the Project Manager for the StolPaN Consortium and Managing Director of SafePay Systems, and he'll talk a little bit about the uptake of this technology in Europe and some of the issues that have been raised over there.

MR. VILMOS: Thank you. I was invited to talk about the European experience, and I will do that, but before I start, I would like to give some
perspective generally about mobile payment and this mobile contactless technology, because it's much more, I guess, than what you are talking so far about.

We have this mobile handset, and we can place a card in it, and that's what you're concentrating on today. But as a reflection, to place one plastic card or one contactless card, one bank card into the mobile handset doesn't really make sense. It doesn't really give much customer value, and it costs a lot for the issuers, as well. So let's start already with multiple cards. Let's put different bank cards -- freedom of choice. Let's put different bank cards from different issuers, Visa or MasterCard, whatever, and then you have the choice which one you want to use.

But besides putting cards, you can also introduce new financial instruments, offline payments, for example. Prepaid purses, micro purses, where electronic money is stored in your handset, and those are again contactless payment instruments.

And I'm talking also about using the mobile as an acceptance device. I know that it doesn't fit with the present security requirements. I'm not talking about open loop payment systems, but for closed loop, small propriety systems, mobile can work as an acceptance instrument.
But if you are talking about mobile payment, you shouldn't just consider proximity transactions; you should also consider remote ones. Because mobile is by principle. It's a device which has remote communication channels. So why not then combine it with value-added functions like mobile banking, new services like sending invoices, making time deposits, making realtime payments using mobiles. So everything has to be considered combined when we are talking about mobile financial services. And obviously, it gives great new potentials, but adds to the complexity and to the challenges.

Now, when we are talking about contactless payments or contactless services, we have to consider that it's not just financial services. As we heard before, for example, in Europe, contactless ticketing, contactless transport is a lot more advanced than contactless payments. So perhaps, or probably, the driving use case in Europe for take-up of contactless mobile services may be the transport industry.

But then it can be loyalty. It can be excess. It can be event ticketing. It can be a number of other services. And depending on the market specifics, in one country it is going to be one service which will lead the penetration; in another country it's going to be a different one.
Now, if we are talking about a static portfolio like this one, this is not very convenient. So we have to give the choice to the customer to make selections, delete existing services and download or deploy or load new services. So it's going to be a whole dynamic environment in the mobile handset, and this is what is the real value proposition.

Now, obviously, the final topic I will be talking about, whether we have the regulation and the legal framework available to secure data, data protection, privacy and other constants, whether we have addressed it already. Obviously not, because that's the future. But when we are talking about legal, open legal and regulatory issues, this is what we have to consider, because this will come. The question is not whether it comes; the question is, when will it come. And we have to prepare for that.

Now, I'm going back now to the original issue of what we are doing in Europe.

Europe is considered to be the most advanced or the more advanced geographic region where mobile communication is, with mobile communication concerns. We have high level of mobile services, and mobile financial services are really getting mainstream. We have mobile banking, different basic or even interactive
solutions. I was just talking to someone during lunch that we can transfer money from our mobile device to merchants or to other people. We obviously make parking payments from our mobile device. So mobile payment is done, not the proximity one, but the remote mobile transactions.

On the other hand, contactless payment is pretty much behind what you have experienced here. We hardly have any contactless acceptance environment, and the primary issue is that the timing is really bad. In Europe, during the past few years, the banks have spent billions of euros on converting their acceptance environment to chip and PIN. Now, it's very difficult to convince them again that, now you are done, great job, now you can start all over again and do the contactless interaction.

We probably should have thought more strategically about it, or it probably was too early, but this is the fact that now we have (inaudible), and it probably will take a couple of more years until we can start a new cycle.

Now, the bad news is that mobile contactless services or the introduction of mobile contactless services is not going to be driven by the contactless industry. It will follow a contactless acceptance
environment. When plastic cards, either transport, ticketing, payment is already on the market, is prevailing, then that's the time when mobile contactless services will really mature and being introduced commercially.

Now, we have heard that we need key stakeholders, and the key stakeholders are the banks and the mobile network operators. Actually, not just the banks but other important service providers, but transport companies. But what we see in Europe, at the GSM associations or the industry association of the mobile network operators, and the banks, the European payment councils are getting together, and within the European payment framework, they are working on joint solution or joint initiative on mobile contactless services.

On the other hand, although commercially the service is not available in Europe, it's going to come. We have multiple trials. We have new trials. You hear it in London with Oyster; that's the subway transport card. Barclays, they have very successful trials there. This is the largest one or one of the largest one in Europe. France is very active. In several cities in France, there are major trials, and those are very unique. I guess those are the most complex ones all
over the world, including Japan, because this is the one where the most players, the most active stakeholders are involved and are incorporating mobile services. This includes multiple mobile operators, multiple banks, retailers, different handset manufacturers, so this is really complex. This is really almost like a commercial operation.

We have very interesting solutions in Turkey, where they combine transport and payment in such a way that you can actually use your payment card for accessing the transports. So at the turnstile, you are not presenting a ticket, but you are presenting, I guess, a Visa or -- I don't know, one of the payment cards, and then it's directly debited from your card, so it's a very interesting solution. Also in Norway, there are new initiatives.

In all these trials, we see very good telco and mobile network operator and bank operations. The problem is that they are pretty much island solutions. There is no interoperation between these initiatives, propriety technology, specific handsets, so there's no way from these specific solutions we will get a European wide, overall, homogenous system. And the solutions always need special technical environments, because, as I said, it is not ready yet.
The question is whether people who are involved in these trials like it and what effect the trials have on the population. I have to tell you that, generally, people don't care about these technologies. We here in this room may be very interested in it; we may like it; we know the benefit. But the general population, first of all, doesn't even know what we are talking about. Second, doesn't care.


(Laughter.)

MR. VILMOS: So that's the reaction of the general public on what we are talking about here. So really, just Forrester, which is a very important -- well, in this industry, it's a well known researching company; they just presented a study that only 23 percent of the population is interested in contactless payment. And even less, only 15 percent, is interested in mobile payment. Now, they also realize that in those cities where there's a contactless infrastructure, like
contactless transport, the reception is a lot higher.

Now, but if you give the choice to the public to try it, then you get completely different fears. In Holland, there was a retail trial, C-1000 is a retail chain, and they operated a mobile contactless mobile trial and they showed different services, and mobile payment was the easiest, and 68 percent of the trial participants, they said they would prefer mobile payment over the cards, over using cards, and only 10 percent said the opposite.

Now, it's more interesting that the satisfaction rate was really high, and 94 percent said that they would really recommend it to others, and around 50 percent, half of the people, they said they would be willing to change their handset immediately to NFC-enabled handset if they would have the choice to keep on using it. And another 44 percent, so this means that almost everyone, said that for their next phone when they would replace their handset, they would be willing to buy an NFC-enabled handset. This is very encouraging, really. But as I said, people who have not tried it really don't care.

Now, more interesting, and it's a message for the mobile operators, first movers may have a commercial and marketing advantage, because over half of the
participants, they said they are even willing to change their network operator if one is offering a service and another is not. And they said that -- this was a trial which was considered really successful, because people were not doing one transaction and another one a couple of weeks later, but they constantly purposely made their payment transactions using their mobile handset. So this is a good sign, but education, as was the previous question, is kind of important.

One interesting story, I didn't put it up here, but there was the question, which is the most favorite feature of your NFC handset? And there were people who said that NFC-based payment in their mobile handset was more important for them than SMS messaging.

Now, how do we see the security consideration, and what do we see about the regulatory issues? From the same study, it was obvious that people cared about security. They would like to have active PIN protection in most of their transactions, even for low-value payments. This is very important that we have to consider when we are designing the system. And we have to take it into account that payment is really a basic environment.

Now, before I start talking about the actual regulatory environment, we have to see that mobile
contactless payment purely from a transactional perspective is nothing different from a contactless payment using a card. An actual contactless reader shouldn't even recognize the difference, whether I place the card or a mobile handset to it. So from a transactional perspective, risks are exactly the same.

Now, as I showed on my first two slides, the environment is completely different. There are multiple operators, multiple services residing side by side on the same secure element, and this obviously adds to complexity, adds to the challenges, and requires new regulation.

Now, with this one, I already answered my next two minutes, but I will be talking about whether we have the regulation in place. We have many laws and directives in Europe on a community basis, but obviously they cannot address all the issues which we will be facing when mobile contactless or mobile payment is going to come. Because as you see, the data, these were issued in 2002, '95, where we didn't even hear about contactless not to mention mobile contactless, so we cannot expect that these laws or these directives are addressing all the issues.

And many other questions we still don't know.

As I said, we have trials here in the States, in Europe,
in the Far East, but in their complexity they are much
simpler than what we will see in the future when,
really, mobile contactless services will proliferate.
So we just need to prepare for it, have to consider it.
And just to raise a couple of issues which
we will actually face, we have privacy solutions,
data protection, but liability is going to be a key
issue.

Now, you have a mobile handset, and we hear
that some of the -- you will store your applications in
a secure element. A secure element may be your SIM
card. So who owns the SIM card? The SIM card is
usually owned by the mobile network operator. Then you
are going to place a payment instrument, the payment
card, into the secure element. Who owns this payment
card? Most of the time, it's owned by your bank. And
the payment card and the SIM card is stored in your
handset. Who owns the handset? Obviously, usually the
owner owns the handset.

So we have an ownership structure and
different parties involved in the issuance of the
application and the operation, so we will have a very
complex environment. There are corporations, liability
issues, that will have to be managed somehow. The same
thing which adds to the complexity that mobile financial
services really makes sense if you can view it on the remote communication potential. Now, I wouldn't like to get a payment card, like today, that you get it in the mail; it's not going to work. So probably all of these instruments, all of these service are going to be shot over the air.

Who has access to your handset? Who can push down data to your handset? How will you manage the remote communication, the remote management of these applications? These are again issues which have to be regulated, has to be discussed, and it's not going to be an issue for a single industry. This will need inter-industry cooperation.

One other thing and I will finish it.

We have the consideration of security. Payment security is always the highest. But as I showed, there are many other services on the same secure element. Transport, loyalty, whatever. Do we really need this same level of security for these services like for payment? Probably not. Will these services be willing to pay the high cost of security? Probably not.

So we will have to find a solution where real high security environments can coexist with services which don't need that high level of protection, doesn't have such an importance in case of privacy and things
like that.

Thank you very much.

MS. RATTE: Thank you very much. I just have one question for you before I throw it open to the group. It seems like we keep coming back to the issue of consumer education being very important in this space. Are you aware of any efforts under way in Europe to let consumers know about what's happening, let them know about the possibilities in this market?

MR. VILMOS: Outside of trials, not really. It hasn't been addressed yet, because the importance, the urgency, is not there yet. So it will come.

MS. RATTE: Even though the European commission has been undertaking this effort for some time to look at RFID technology specifically and assess the need, has that sort of spurred interest in it?

MR. VILMOS: Yes. RFID, in general, as the technology is addressed, is debated, is discussed, but the specific mobile aspects, the mobile services, RFID in general is in a more advanced state than mobile services.

MS. RATTE: Okay. Now, I'd like to throw it open to the audience. And anyone who has a question, I'd like to ask you to identify yourself before you ask it. So do we have any questions from the audience?
MR. MOORMAN: Dave Moorman, Director of Retail Technology for PCMS.

My question is, what is the mobile payments industry doing in terms of securing this little device here? What I'm seeing is, these are increasingly programmable devices, and a lot of these schemes I'm seeing are based on the idea that this is a black box, and it's running software that the mobile phone company has loaded on it and that they're maintaining, but I'm betting that eventually you're going to have viruses inside of this thing that are going to corrupt the programming inside of this, and so now it's going to do the will of whatever that virus is. So what is the industry doing to make sure that this doesn't become another Microsoft Windows?

DR. NARENDRA: My take on that is, I think most security solutions, as far as I know, are always reactive. You can be as proactive as you can based on what you know, but you have to be able to react as soon as you can. So there isn't a magic bullet that says this solution will solve the problem for securing this device. The moment you open up the architecture and have additional services from being just a phone to everything other than cooking, it does open up issues and you just need to be proactive -- well, you need to
be proactive and, actually, more importantly, reactive
to security issues.

MR. WAKIM: I can add from a mobile platform perspective. Unfortunately, we're going down a little bit the same path as the PC. There are mobile antivirus software available, and it's one of the most popular applications that is purchased on smartphones.

Companies like F-Secure, for instance, make mobile antivirus.

MS. RATTE: Any other questions?

Okay. I've got one I can throw out. Coming back to the question of messages to consumers, who do you think -- you know, each of the panelists has sort of hit on the fact that this is a space with a lot of different players in it. You've got the mobile network operators; you've got the banks, card issuers. You know, it's a complex space. Who do you think is in the best position to give messages to consumers, and are we in danger of giving consumers too many messages and maybe conflicting messages?

MR. HANSEN: I'll take that one. I think it depends, and it depends on the particular implementation. But in the end, the consumer will be a customer of one or more service providers, and it will either be a customer of the wireless carrier, be a
customer of a bank, be a customer of a transmitter, may.php
be a customer of an aggregator, taking a portal model;
you might log into a portal like you do on the Internet
today and access other services.

And one way to think about it is that the
company who owns the customer relationship has an
obligation to inform consumers, and often it's going to
be a shared responsibility. And this is a complex
product. The parties will need to cooperate in order to
launch it successfully, because it's by definition
mobile payments. It blends at least two parties, maybe
several. And so they might come up with things like Web
sites with FAQs. They might have terms and conditions.
There usually will be end-user license agreements and
other click-through agreements in the software. There
are other ways to do it, but I think it's a shared
responsibility, and it will become apparent in the
actual business model, I think, who has the ultimate
responsibility for that.

MS. GRANT: Just a quick comment. I think
that it's very important in that all the stakeholders
have a role to play, but my hope is that there actually
wouldn't be that many messages that we have to get out
to consumers, that a lot of the things that will protect
them in this space will be built-in and automatic so
that they don't even have to think about it, they don't
have to understand it. They're never going to be
techies. And it's all the same issues that we deal with
right now with PCs. It's just got to be made really
simple and built-in and automatic for consumers to use
it.

MR. VILMOS: I agree with you, because we
have to be really a foolproof, simple, but secure
environment, but otherwise it's not going to work. On
the other hand, we should avoid frightening the
customer, because obviously there are risks. We may not
even have identified all the risks that there are, but
by the time it's going to be out there, it's going to be
mainstream, most of these issues have to be solved;
otherwise, it's not going to work.

So this is, I guess, the approach we should
start. We should discuss the problems, should try to
understand and identify the problems, but definitely
should avoid bringing up risks which are not real but
which are good enough to frighten the general public
who don't know beyond the real details of the
technology.

DR. NARENDA: I have a short comment. In
terms of the responsibility of consumer education, it
will really rest on whoever is making transaction fees.
So in that sense, it depends.

I'm not 100 percent certain when it comes to mobile payments in steady state whether that responsibility will be shared. I'm not 100 percent certain. I would prefer it not to be, but I may not have a choice there.

MS. RATTE: We have one more question. And could you identify yourself before you speak.

MR. JOHANSON: Eric Johanson, the Schmoo Group.

So within just the wireless payment system that's here in the U.S. that's currently deployed, we have a billion different names for it, right? It's EMC, it's Tap & Go, it's Swipe & Pay, it's Blink & Pay; it's got a million different names that we're seeing. I think this is one of the primary issues that's confusing consumers in the marketplace, because there are several standards for logos and things of this sort. But there's a million different competing products for access control and proximity cards, as well as transit tokens, as well as payment solutions, some of which are compatible, some of which are not, but even the compatible products have different names. That certainly doesn't help consumer acceptance.

MS. RATTE: Thank you. Anyone else, any
final comments?

MR. CECHETTI: Hi, my name is Adam Cechetti, also with the Schmoo Group. Just a very quick comment. There are already mobile viruses, and that's why you have mobile antivirus. But there's not many, because there's not much advantage to putting a virus on your cell phone. As soon as you start pushing payments and other complexity things to there, you're going to see that space explode. And many of the cell phones that are being designed today don't have adequate protections to be retrofitted to be moved forward to actually secure that environment correctly.

MS. RATTE: Thank you. I think we're going to break a little bit early. It's 3:15 now, and we were hoping to start the next panel at 3:30, so please join me in thanking this excellent panel.

(Applause.)

MS. RATTE: And we'll see you back here at 3:30.

(Recess taken.)
MR. HARWOOD: All right. We're going to get started. For our last panel of the day, we're going to be discussing Meeting the Challenges: Strategies and Approaches. And our moderator will be Professor Bill Covington from the University of Washington. You'll find information about Bill in our bios, as with all the other folks who have spoken to us today.

I'll just note that we are here in this room and we are enjoying the hospitality of the University of Washington thanks to Bill's efforts, and we're grateful for those, and we appreciate the opportunity to work with your students and with your building, and particularly with you. So, thank you, Bill.

MR. COVINGTON: No, the pleasure is ours. I was a little nervous that the information about me might be found in the post office. But thank you all for coming. I think we've had some very dynamic sessions.

And while contactless payment systems offer numerous benefits, there are also potential challenges, and I believe this panel is going to explore some of those challenges and possible solutions.

There are a number of basic questions that need to be refined, posed, and answered when it comes to the use of this technology. Some of those questions...
might be:

What are the legitimate expectations of the customer who makes use of a contactless payment system? What should they expect in terms of the capturing of the data during the initial transaction, the transmission of that data from the point of purchase, and what are the responsibilities of those who possess and store the data? What can the customer legitimately expect in terms of accuracy, security, access?

A second question might be, what are the rights, duties and expectations of those organizations that are part of the contactless payment system? What information, if any, should they provide to the customer? Should they be held to a 100 percent standard when it comes to security throughout the system? What, if any, relationship should they have with regulatory bodies?

Other questions have to do with the current state of the law: Do we need new legislation? Do we need new regulations? Are our existing laws adequate?

I took the liberty of Googling the names and the organizations of our very distinguished panelists, and I will try and give a little interesting informational tidbit to start with, and then we will be hearing from our panelists from my right on down.
First, we have Alissa Cooper, who is the Chief Computer Scientist for the Center for Democracy and Technology. According to their Web site, CDT works to promote democratic values and constitutional liberties in the digital era. With expertise in law, technology, and policy, CDT seeks practical solutions to enhance free expression and privacy in global communications technologies.

Ms. Cooper.

MS. COOPER: Thank you. And thank you for hosting today, and thank you to the FTC for inviting me out here. I think it's been a really enlightening day and one of many of my favorite FTC workshops that I've been to.

As Bill said, the Center for Democracy and Technology is a nonprofit public policy organization focused at the intersection of civil liberties and digital technologies, and one of our core values from the beginning has been consumer privacy and putting consumers in control of their own information. We really harp on this all the time, that consumers should have the right tools that they need to be able to manage their own data.

I'm going to start with a little story, and it sort of builds off of Dr. Fu's story from earlier
about the engineer who didn't know that he had a contactless payment card.

I met last year with some of the card issuers to learn more about contactless payment and how the technology was working, and it was a good meeting; I learned a lot. I learned about some of the features that I thought were very helpful, that the card needs to be close to the reader, that there are these dynamic, what I will call CVX values -- choose your favorite last letter there -- but these dynamic values that also get transmitted during transactions.

But I was a little bit concerned that names and card numbers and expiration dates were also being transmitted. To me, that seemed like a possible loophole for privacy invasions. And about a month later, my credit card expired and I got a new card in the mail, and it was contactless, and it had the symbol on it; I realized that it was contactless, and I thought to myself, you know, me being a privacy person, well, should I put it in the microwave? You know, should I get my sledge hammer? And I figured that maybe the card would come in handy to me in the future, in its working fashion, so I decided, you know, I'll put my name and my credit card number out there, perhaps, and hope for the best, in the idea that this might come in handy at some
point.

And I actually tried to use the card, as well. There's a drugstore near my house that I noticed after a few months had installed these contactless readers, and I went in there and I tried to use it, and it didn't work. I couldn't seem to get it to work. And actually, this isn't the card, but after a few times, you start to feel a little sheepish. You go up to that reader, and the cashier is kind of looking at you like, what on earth is this woman doing? And, you know, doesn't she know how to swipe her card? And I tried it a few different times and nothing ever happened, never got the beep that Jennifer was talking about this morning, I didn't get any sign that it was working, so I'd just quickly turn it around and swipe it and be on my merry way.

So on the one hand, I kind of thought to myself, well, maybe I never needed to put it in the microwave because it doesn't transmit anyway, and I sort of forgot about it. But that was last year. Now, this year, the FTC workshop came up and I decided to try again, and I noticed there's a really upscale grocery store that opened a location near my house, and I went in there last week, and, lo and behold, the card works. So I realize, I guess, this whole time that my personal
information has been a little bit vulnerable.

But I guess the moral of the story is, I was a person who was well versed in the technology, I understood it, I understood how it worked, and I still had that experience where I went to the store, I couldn't figure out what was going on; I certainly could not ask the cashier, because she obviously had no idea what was going on with the reader, and I sort of thought I had extra level of protection, but then it turns out that I don't.

And I actually called my bank and I talked to them about it for a little bit, and they said, yeah, it's probably a problem with the retailer. And I was like, okay. But I just think it's a useful anecdote that I was thinking about when I was preparing for this.

I've split my comments into kind of four categories, and I'll focus really on the first two for the most part.

The first one is security. We've heard a lot about security today. And to me, I think the big take-away of today is, we should really be forward looking on security. In the previous panel, we talked about being reactive versus proactive, and I think they're both important, but there are some things that we know about security based on our experience with
digital systems over the past decades.

I'm really surprised that, thus far, this example hasn't come up with the MIFARE card, which is, there's two billion of these cards in the world, it's the most popular transit card in the world today, and there are three separate researchers who last year published their results of their research showing that the card could be attacked, quite easily for them, at least. And in recent weeks, the company that manufactures the cards sued one of the researchers in order to not have some of the research published, because the algorithm that they used to secure this card was secret, and this was part of the security of the card. It had a secret algorithm and it also had 48-bit encryption keys on the card.

Now, to me, thinking about this in 2007, the fact that the most popular transit card in the world is using 48-bit encryption keys and security through obscurity, which are both things that I feel like everyone in the security community has learned that these things just don't work. And I feel like we really need to think about leveraging all of the experience that we've had, whether it's in the PC world, whether it's in the financial services world.

We've been through some of these lessons many
times, and we should think about that moving forward. This may be a new technology, it's different, you know, you tap the card instead of swiping it, there's many differences about it, but some of the underlying security protections should be the same.

And it's the same I think with mobile, and I've been reading about fishing attacks that use NFC. So you hold your mobile phone up to one of those smart posters that the gentleman from Nokia was talking about earlier, and it directs you to a malicious Web site and tries to get you to input your credentials. Exactly the way that fishing works on the Internet, but now the vehicle is contactless and you're holding your phone up, but it's the same attack vector. And so I think in designing these systems and looking towards the future, we should really leverage our previous security experience.

And I also feel like today we've heard a lot of consensus, actually, about what some of the good security practices are, and I'm wondering in my mind if there's some role for uniformity there. You know, we heard about not transmitting names, which seems to be an emerging best practice. We heard about having random or dynamic data transmitted with the card, and I would say the best practice really is to have as much of the data
transmitted be random and dynamic.

We've heard a little bit about having transaction counters, so that if you could do a fraudulent transaction, it would only last for one time. We've heard about having the shield on the card when it's sent in the mail, and a little bit, Mark McCarthy talked about card and reader authentications so that a rogue reader wouldn't know how to authenticate and wouldn't be able to read a card.

I feel like all of these things, and there were many others that were touched on today, seem like, to me, emerging best practices, and I'm wondering if there isn't some way for the industry at large, the industry groups, PCI, Smart Card Alliance, FTC, I don't know what the right home is for a set of standards, but it certainly seems like there are some standards, and to a consumer who can't really tell the difference between one card and another and whether one card is a CVV or a CV3 or whatever it is, it seems like having a baseline uniform set of standards could be useful.

Now, on privacy, I feel like we've heard a lot about choice, and I completely agree with those who spoke earlier who said that you should be able to refuse the card; you should be able to -- if you get a contactless card and you don't want it, you should not
be forced into using it. And it's good to hear that some banks are offering that option, but I feel like that's another thing where it's just like, seems like should be universal.

But I also think on choice, we really don't want to foreclose the ability to do anonymous payments, and if contactless is the only choice, then we've lost that, so that's another aspect of choice that I think we need to keep in mind.

And then as far as mobile is concerned, thinking about privacy, the gentleman with CTIA was talking about consent, I think even when you have choices and you decide, yes, this is something I want or, no, it isn't, it shouldn't be consent once and it's forever. So if you buy your mobile device and you have to decide, yes, I want to use contactless payment and therefore every time I make a payment that information is also going to go to the network operator or it's also going to go to some application on the phone, that's not true choice, because you're either saying, I can always -- you know, every time I pay for something, this information is going to get shared, or I just can't use my phone to pay. So I think when we're thinking about consent and choice, we need to think about true choices and not this kind of false choices where it's all or
nothing.

The last panel touched on interoperability, and I think as we think about mobile payments, in particular, it's going to become extremely important. There's a million different SIM cards out there, a million different memory cards, a million different device makers, and it's not going to make any sense for consumers to have to open a new bank account every time they want to get a new phone, or, you know, to not be able to take their account from phone to phone. These are huge barriers that I think could stand in the way of some of the benefits that mobile payment provides.

I think the comparison to the Internet and kind of the open development model on the Internet is a useful one. You can think what you want about how open mobile networks are, but they certainly have not seen near as much innovation in the application space as we have on the PC side and on the wireline broadband side. And so I think it's important to think about which path do we want to go down, if we want to continue to kind of pursue the closed network model, or if mobile payment can sort of be a vehicle to convince the mobile network operators that a little bit more openness will actually promote consumer acceptability of mobile payment.

I think on consumer education -- my fourth
point is consumer education. I think we just need to think about the way that consumers use their current payment and the way that they use their phones. So are you going to remember to cancel your credit card when you lose your phone? Are you not going to be able to pay for things if you leave your phone in the cab? Are you going to give your keys to the valet and have him go run up charges because you just handed him your credit card by accident? You know, things that you would never do. And I think, as Susan touched on earlier, are you going to buy a mobile phone for your kid and thinking that, oh, this is great; now he or she can call me and tell me where they are or where they are in the world, not realizing that they're flashing it around to every reader and buying all those things that you never let them buy.

So I think we can think about consumer protection issues kind of broadly and miss the idea that there are some mental models that all of us are very used to having, and there's going to be lots of these weird situations where it's like, whoa, my credit card is my phone; you know, what does that mean for me as a consumer?

Finally, I would just say, as always, the good actors end up on these FTC panels, and I think, you
know, we heard this morning Wells Fargo had a choice, should I take a more secure option, should I take a less secure option; and they took a more secure option. But the people who aren't up here are the banks that don't offer choice or the merchants who are not making use of the security features, and as we think about what to do going forward, we need to think about the less than good actors and not just the folks who are willing to come to forums like this and talk all about all of the great things that they're doing for consumers, because we all know that it's a wild world out there and there's lots of other players in this space who are not necessarily meeting up to the practices of the folks that we've heard about today.

Thanks.

MR. COVINGTON: Thank you.

Dr. David Moorman is Director of Retail Technology for the PCMS Group. And PCMS is one of the world's leading providers of software and services covering the whole of the supply chain, enabling retailers and distributors to manage their business. And I believe Dr. Moorman is author of "Integration without Boundaries: Using Standards to Connect the Enabled World."

Dr. Moorman.
MR. MOORMAN: I think we got some confusion on speakers. I'm not a doctor, and I didn't author that paper.

MR. COVINGTON: And I teach hi-tech.

MR. MOORMAN: Well, thanks to the FTC for having me here, and thank you for the promotion to doctor.

MR. COVINGTON: I do it all the time.

MR. MOORMAN: We did get the title right. I am the director of Retail Technology for PCMS, a global point of sale, primarily software, vendor. And I'm also wearing another hat, actually several hats today. One is as the director of technology for that company. That company, we're the point of the sword. We're the piece of software that sits on that device and takes that information from the consumer and then passes it along the stream. So that's very much the emerging standards, and where this is going is very much of interest to us.

I'm also a member of the Association for Retail Technology Standards, ARTS, their governing technical committee. And ARTS is a division of the National Retail Federation. So I'm involved in the development of standards. And ARTS is mainly about efficiency standards, how to make data flow from one retail application to another, not so much compliance.
But one of the things that PCMS and ARTS work together on is a very successful standard called Unified Pause, U-Pause, which is the programming standard for retail devices. So when you swipe one of those legacy magnetic stripe readers, that data, that track data is passing through a standard interface that was designed by those two entities. So we have a lot of stake in this game.

I'm also here as a consumer, and I'm also going to tell my consumer story about credit cards.

In fact, it was a coincidence, the day I was asked to be a panelist I got a call from one of the credit card companies -- which one was it? Which one of you guys? It was MasterCard, and they said my card was making the rounds buying televisions in Bangalore, India, and were these valid transactions. And I said no, and they voided the transactions; they actually hadn't gone through.

But for that day, I was an un-person. They said they'd overnight me a new card. And I was out traveling, and all of a sudden I found out I had to go back and put a different credit card, fortunately I had one, on the hotel room bill and a number of other things. I had to get online and do a whole bunch of stuff so my life wouldn't come apart.
Coincidently, a few months earlier, I had been to a grocery store, to a self-checkout, and I took out my wallet and I laid it down while I scanned my items, and the disabling device that disables the theft protection, like for DVDs, wiped out every magnetic stripe in my wallet. And again, I became an un-person. All of a sudden, I was not able to transact business; I wasn't able to prove who I was. This is an example of what I call Type 2 incident theft.

I think we've talked a lot about Type 1 identity theft, which is someone else stealing my identity, but another type of harm is this Type 2, where I can't be me because of the actions of another party.

My point here is that real people are getting hurt.

And one of the other stories I always tell my nontechnical friends in trying to explain what I do in the job is, I always point out the old science fiction movies or the old James Bond movies where they overload the computer and smoke comes out and it bursts into flame and glass flies all over the room. And I always tell them, I almost wish that happened; I almost wish when computer systems didn't work, they would just explode. Then it wouldn't have taken us ten years to
get a version of Windows that doesn't lock up.

Again, all due respect to the building.

My point of all of that is, real people are getting hurt, in real ways, and consumers, and I think that makes it appropriately the FTC's business to get involved. And I predicted to the management of my company a year ago, watch the FTC, because it's going to happen.

Although I'm not going to talk extensively about contactless payments as much as other people have, I'm going to talk about more approaches and some of the things I'd like to see the FTC doing. But we've already talked about the fact that it's already here. If you've got a cell phone in your pocket, some computer out there in the world knows just where you are, and that information can be queried.

So it's not a matter of if, or if ideas can happen, it's when and, in fact, it's already happened. We can either figure out how to regulate this smart, or else it will end up getting regulated stupid. Let's not wait until two senators get their name in the paper about the privacy issue and pass some act that is going to make an emergency measure of getting a handle on this topic. One of the big keys here that we've got to work towards is balancing innovation against standards, and
one of my themes is, where does the standards community play in this whole thing, and what is FTC's role in that.

Another story: I got pulled over by a police officer once, and he said, you know, you're driving on the wrong side of the road. And I said, no, I'm not not; I'm an innovator.

So my point is, somehow we have to have this balance against what is society -- what standards do we need to make society work and make all of this work for the consumers and without derailing innovation. And my concern is, at some point if this becomes a senior political issue, that we're not going to have the time then to make that proper balance between innovation and keeping the economy going.

Some of the drivers and things I've heard this morning that as a technologist kind of jumped out at me and I said, well, I don't know if I buy that. One is, phones are programmable. To use the mobile payments as an example, these are devices, they've got a little operating system in there, and it's a matter of time, in fact it's already happening, that viruses are going to get in there. And as somebody pointed out, once money becomes a motivating factor and not just annoyance, the viruses will explode.
I'd like to point out that there is a large body of hackers out there. I do a lot of training and a lot of consulting, and a lot of the people I'm training, for example, for the implementation of my product, are offshore developers. We are training a small army of offshore programmers in how these systems work. And Alissa used the term "security by obscurity." There is less and less tolerance, and there must be less and less tolerance against the idea of, oh, well, nobody will get in there and figure out that microcode or how to do that buffer overrun. That's been proven time and time again that that's just not obscurity -- security through obscurity is just not security.

I heard some things about proximity: Oh, well, you have to get it two inches from the reader. That goes right up there with another of Mr. Gates' comments: Nobody will need more than 64K of RAM ever.

The only thing that is true in life is three things: death, taxes, and the miniaturization of IT. And something that can only be read from two inches away today will be readable from two miles away tomorrow. So we do need to be forward thinking about what is the technology turnover rate.

And one of the things there is, and I'll talk more about this in a minute, to represent the merchants'
viewpoint, merchants have very ponderous infrastructures. It's very expensive for them to turn over their technologies in store. So I hear people say things like, oh, all you've got to do is apply this patch, or all you've got to do is put another 128 megaRAM in there. Well, it's not the cost of the 128 megaRAM; it's the cost of sending somebody out to the store and opening up the box and putting all that extra memory in there and dealing with all the issues with drivers and whatever. So any mistakes that get made in the implementation of these infrastructures, retailers have to live with and have to amortize those costs over a very long period of time.

I want to talk a minute about an article and some of the things that came out of it. I encourage you to go Google this. There is an article out there by Information Week called "PCI and the Circle of Blame." "PCI and the Circle of Blame." It was published in February of 2008, and it gives a really good overview of the liability and political issues swirling around PCI and the liability.

Coincidentally, a month later we had the Hannaford breach that you've heard about some. What was significant about the Hannaford breach, a grocery store on the East Coast? Several things. One is, they were
PCI compliant. They had the stamp of approval. Yet they got breached anyway.

The other thing about it is that it wasn't one breach of 4.5 million credit cards. It was 4.5 million breaches of one credit card at a time. And I've heard several things up here about, well, we're not worried about the one-offs, the one-card breach, because that doesn't scale. Well, yeah, it does scale, because what somebody did is they penetrated the system, they inserted a Trojan that listened between the point-of-sale software and the acquirer software and picked up that credit card as it traveled through the memory of the computer. Very innovative attack. Somehow, somebody used a virus to propagate it, so it was actually -- it wasn't somebody hacking into the big data center in the sky and getting all 4.5 million credit cards downloaded; it was a little thing that was listening to every single transaction and sending out those credit cards over a period of time.

So look at that article, and it talks very much about the circle of liability that's forming. I happened, by the way -- in a previous life I was originally an accountant and an auditor, a financial auditor, so I know the world of auditing and the requirements that auditors have as far as
professionalism and doing their job for their clients. And I guess there's no nice way to say it; PCI and the auditing, because of the Hannaford breach, is kind of in a mess right now, because everybody is trying to figure out, what does it mean? Is Hannaford off the block because they were compliant? Well, what is the liability for the QSA? So everybody is trying to figure out what this circle of liability is going to be. It's nice that there is a feedback loop, but right now it's very inefficient and it's very unpredictable. So retailers are kind of flipping a coin as to what to do and how to invest in fixing this problem.

I'll also make note that PCI is a great start. I should note that pcisecuritystandards.org, although it's an org, it came out of the PCI world, out of the payment card industry, and so it's done a lot of fine work, but it doesn't, in my opinion, accurately reflect all the stakeholders: the consumers and the merchants and the credit card industry.

So I talk about the merchants and some of their quandaries and some of the things they've got to worry about. Well, I already said they have ponderous infrastructures, so whatever gets put out there in thousands of stores, they have to live with and they
have to eat the cost if there's patches or upgrades that
need to go out.

Something that was mentioned earlier was
signature capture versus not signature capture for items
over $25. We have the problem of employee -- our own
employees can be our biggest security vulnerability with
employees pocketing cards, skimming, those kinds of
things.

Do we go contactless or not? We have to deal
with offline issues. The network isn't ubiquitous to
the point where you're always online. Retailers have to
make a decision: When the network is down, do they take
the credit card and hope it's not a fraud? What do they
do there? I deal with those issues every day.

What I'm tying to get at here is, merchants
are in a really tight bind right now, because they have
to compromise between service level and security. And
each retailer has to kind of guess where they want to be
on that spectrum.

To use an example, compare this to an
airline. We would never say to the airlines, it's
entirely up to you whether you do maintenance or not or
whether you put gas in that airplane or not. We don't
let people in the airline industry play with people's
lives, and what we need is -- and I'll get to my point
in a moment about standards -- we need to make the
retailers, help the merchants get off the hook by giving
them clear standards that everybody is going to play by.

I'll go on and come back to that.

I'd like to look at other regulatory models
that have worked. I use my plane analogy. We have a
National Transportation Safety Board that looks at
problems. Whenever an airline goes down or there's ever
a problem, the NTSB, as a third party, investigates and
says, what went wrong? Their job is to say, where did
the breach occur based on certain standards that are
previously set? And over time, for all of its
disadvantages, our airline industry is actually pretty
good. I mean, most of the time, I looked it up, there
are about 50,000 flights a day in the United States, and
they almost never crash.

In the appliance industry, we have
Underwriters Laboratory, which certifies our appliances
so they don't burn our house down. So there are many
regulatory frameworks out there that I think we can
learn from. And one of the things that I think is
lacking in IT in general, and particularly in this area,
is the ability of arbitrating what is a foreseeable
versus a not foreseeable problem.

If you're familiar with Palsgraf versus Long
Island Railroad, in 1928 it established foreseeability as the standard for liability and negligence. We don't have anything yet where we can definitively say, when something goes wrong, how are we going to go in there and figure out who really is responsible for that breach.

Microsoft has a really good term for this. They call it surface area. What is the surface area of the system. They take it from stealth. You've got an airplane, and then when they came out with stealth technology, they said surface area is now much smaller than the actual airplane. Now it's the size of a sparrow. And what we need to do is come up with a regulatory framework that will over time reduce the surface area for these army of hackers to get into.

To recap, there are people who are really getting hurt; that makes it the FTC's business. We have to balance innovation against keeping the economy going. And we have some established regulatory models.

And I'd like to make a call to action. I'd like to see the FTC get involved in bringing all of the parties to the table and all of the stakeholders to the table to compel some standards that have some muscle and some teeth to it. We saw many cases up here of "he said, she said," of, well, you can't get a PAN off this
thing. Well, beep, there it is, and can that be used for creating bogus credit cards.

Whenever you deal with security, you have to talk about what are all the different -- security isn't one thing, you have it or you don't. You have to talk about what are the different access threats, and that can become a very emotional argument. I think FTC has to come in and be involved both proactively in the role of standards and reactively in the role of forensics, to start to bring some accountability to the situation.

It's a journey we're on. It's a journey we all need to take together. But we've got to move that surface area smaller and smaller incrementally in real ways.

And my time is up.

MR. COVINGTON: Thank you, David, and my apologies for the errata.

Kathryn Ratte is Senior Attorney for the Division of Privacy and Identity Protection with the Federal Trade Commission.

Kathryn.

MS. RATTE: Thank you. And my apologies to everyone in the room who has to listen to me on two consecutive panels. I'll try to keep my remarks brief.

I'm here to now to give you a very brief
overview of the Federal Trade Commission and how we
address issues raised by emerging technologies through
our existing enforcement authority.

If there's one message I want to leave you
with, it's that the FTC has the tools to address this
type of emerging technology and others using our
Section 5 authority, which is broad and flexible, and we
are out there on the beat, and when we see practices
that deceive consumers or harm consumers, that's when we
step in. So now would be a good time to give the
standard FTC disclaimer.

The views I'm expressing are my own and not
necessarily those of the Federal Trade Commission or any
individual commissioner.

So, as I mentioned, we're an enforcement
agency, and our responsibility includes enforcement of
laws related to data security and consumer privacy, and
these are very high priorities of the Federal Trade
Commission. Although my focus today is on law
enforcement, that's just one piece of what we do. I
wanted to mention that we do take a multidisciplinary
approach to protecting consumers. In addition to
rigorous law enforcement, we conduct outreach directly
to consumers to give them the tools to protect
themselves against emerging threats, and we also provide
guidance for industry to help them understand their
obligations under the law.

So getting back to the law enforcement,
although we enforce some sector-specific laws in the
area of privacy and security, including
Gramm-Leach-Bliley, our primary enforcement authority
comes from Section 5 of the Federal Trade Commission
Act, which broadly prohibits unfair or deceptive trade
practices. And the Section 5 authority is very broad.
We reach a wide range of industries, with some notable
exceptions, including the banking industry, and I
believe John is going to give us a little bit of an
overview of what the regulatory landscape is for banks,
but that is one area that we do not regulate. We get
just about every everybody else under the sun.

In the privacy and data security context, the
FTC uses its Section 5 authority to make sure that
businesses keep the promises that they make to consumers
about their privacy and data security practices. That's
kind of the deception piece of our statute. And also to
address business practices that cause or are likely to
cause harm to consumers, including the failure to have
reasonable security measures in place to protect the
privacy of sensitive consumer data. So you can't
deceive consumers and you can't harm consumers. That's
Section 5 in its very, very most basic summary.

Because our deception and unfairness authority is so broad and flexible, we frequently find ourselves at the forefront of new technologies, like the one we've been discussing today, also others, and our standard in this space is reasonableness. We require companies to have reasonable security, to have reasonable privacy practices.

So, accordingly, this means that we can address emerging threats without technology-specific regulation. We're looking at the overall reasonableness of a business' practices, not whether they have one specific security measure in place or, you know, one magic bullet. We realize there isn't one, and we wouldn't be in the best position to go out and anticipate that, anyway. We're looking at the totality of what they're doing for privacy and data security.

I'll give you a couple of examples.

In 2005, we brought a case against BJ's Wholesale Club, which is an East Coast discount warehouse. For those of you West-Coasters here who haven't heard of BJ's, it's like a Sam's Club. And they experienced a major security breach in which the credit and debit account information for many of the customers who had shopped at its stores was accessed by a hacker.
And in that case, we alleged that their security practices as a whole were unreasonable and resulted in harm to the consumers whose accounts were compromised. We alleged that BJ's has failed to take into account the specific security risks posed by, among other things, the use of an unsecured wireless network at its retail stores. Their failure to secure the wireless access points is what allowed the hacker to go into the system and get access to that card holder data. We were able to allege that this failure was an unfair business practice because it resulted in the harm to the consumers.

We had a more recent case announced in March of this year against TJX, the TJMaxx discount closing store. In that case, hackers were able to obtain the credit and debit card information of approximately 450,000 TJX customers that were stored on the system. And again there, the FTC alleged that TJX failed to implement reasonable security measures to protect the customer information it collected and stored, including failing to implement readily available security measures to limit access through the wireless access points at its stores.

So in both cases, the wireless issue was one of a laundry list of security failings. There were also
issues about storing card holder data beyond the time that they should have been, and there were encryption issues, as well. It was really a failure of the entire system.

But I use those to illustrate the point that we didn't need a specific regulation saying you need to secure wireless access points. Because we look at the totality of the system, we can address these risks to consumers as they come up.

And I also wanted to echo a point that was made earlier, that the point of collection of consumer data, which is a lot of what we've been talking about today, the contactless card, the first read, that's just the first part of the whole data life cycle. When the FTC looks at a company's practices, we don't just look at how is information collected, but how is it stored, are there access controls, is it disposed of securely. You know, we look at data retention issues. That piece of it is the start of a whole process, and we expect to see reasonable security throughout the process.

I'll just close by saying that the FTC has been monitoring the potential impact of technologies such as RFID and contactless payment on consumers, and we won't hesitate to use our existing Section 5 authority in appropriate cases if we become aware of
practices that deceive consumers or otherwise harm them. And I'll leave it there, and look forward to your questions. Thank you.

MR. COVINGTON: Thank you, Kathryn.

John Carlson is a Senior Vice President with the BITS/Financial Services Roundtable.

John.

MR. CARLSON: Thank you very much. It's a pleasure to be here. I also want to thank both the FTC and Bill Gates' father, whom this building was named after, because if it weren't for Bill Gates, BITS would not have been established over 12 years ago, and it was in response to a comment he made to a group of CEOs where he referred to bankers as potential dinosaurs, and I saw earlier in the day we had a funny Far Side graphic of a dinosaur smoking. And I think that brings together to me a number of different themes that are important for this event.

One is the role of regulation and where it has limitations and where it's very effective.

Second is, there's a very strong role for the industry to solve the problems and to address the issues at the forefront.

And then third, there is longer-term strategic issues which you really need to keep in mind,
in building on what Dave Moorman had to say regarding innovation, that you can't be so fearful about how the technology could be used in nefarious ways that you don't allow it to move forward and gain some of the benefits that are out there.

And I think Dr. Littman pointed out the important point of costs and efficiency and things of that nature. And our industry, our society, is becoming so squeezed in terms of trying to eke out additional efficiencies and gains that are out there as we have the capacity to do that, so it's important not to hamper ourselves in terms of moving forward.

So let me first talk a little bit about -- first let me explain what BITS is, since many people don't know. We are associated with the Financial Services Roundtable. We focus on the technology issues that affect our member companies, which are the hundred largest financial services of banking, insurance, and securities. We have over the years focused an enormous amount of attention on security, on fraud reduction and identity theft. We actually established about five years ago an Identity Theft Assistance Center which helps victims of identity thefts to restore their good name.

We also focus on outsourcing and vendor
management related issues, which when we're talking about this, we're really covering all three of those areas: security, vendor management, and fraud. And we have experts in our member companies that gather together on a regular ongoing basis to talk about how do we solve these problems. And invariably, we spend a lot of time trying to figure out, well, how do we work with our critical partners, since many of these problems cannot be solved by an individual company; even if you take a very large company like a Citigroup or a JPMorgan Chase, there are issues that have to be resolved on an industry wide basis.

And so we spend a lot of time -- in fact, we spent a great deal of time out here in the Seattle area working with Microsoft on software security related issues several years ago. We've tried to work with the Internet service providers on things having to do with fishing or e-mail authentication and things of that nature.

So there's a really important role, both in terms of what the industry can do to come together to try to solve some of these issues and problems, and there's also an equally important role for government to be thoughtful. So I must hand it to the FTC for holding this forum, to bring people together to talk about it.
I also would encourage the FTC to work with their peers within the broader government in terms of the Federal Communications Commission, the financial regulatory agencies, because each of those bodies have important roles to play. Even though the FTC doesn't have, as Katie mentioned, oversight over financial institutions, it does have oversight of the service providers that financial institutions rely so heavily, both in the United States and increasingly around the globe. So everyone has a role to play in terms of trying to move this forward.

Let me talk about regulation. The financial services industry is, without question, the most regulated industry in the United States. It's regulated both in terms of safety and soundness, and increasingly on operational risk, which includes information security and fraud and consumer compliance and things of that nature.

The regulators have built upon what I believe is a very solid foundation in the law the Congress passed in 1999, the Gramm-Leach-Bliley Act, which the financial regulators took a very bold step in terms of developing a rule that was risk-based, that was flexible, that was kind of a continuous improvement theme in terms of how do you solve this problem, that
it's not going to be a one-shot deal, it's going to be an ongoing basis. And at the time, the OCC was one of the authors of that rule, so I'm very proud of it in terms of I think it's had a prominent staying power.

The regulators have also done a lot in terms of trying to come up with more flexible guidance, supervisory guidance. They're not regulations, even though the industry often times responds to them as if they are. An example of that would be a few years ago, authentication guidance, which said you must enhance the authentication. Many people interpreted it as you must have two-factor authentication, although that's not exactly what the regulators said.

The regulators have also over the last 15 years been thinking about what sort of impact electronic money and banking will have on law enforcement, supervision, the actual manufacturing of money, things of that nature. And so in preparation for this, I actually went back to a conference that the Treasury Department had sponsored with all the Treasury Bureaus, which in and of itself was a unique experience in terms of having all the Treasury Bureaus work together, and they developed a conference and a paper in which they laid out in the paper the following quote:

Government must be careful not to overreact
to or stifle new innovations that can greatly benefit
the consumer and the American economy. Government
should take advantage of marketplace solutions to issues
where appropriate. To do this, and at the same time to
be in a position to act appropriately, it is important
for government to maintain expertise in electronic money
and payments developments and to consider carefully
major questions presented by these developments.

And I think that still holds in terms of
thinking through this problem. We can't be fearful of
what the consequences might be, but we need to be
forward thinking in terms of how these technologies may
be used in unintended ways.

So my conclusion from listening to today's
panel is that the issue of contactless payments is
somewhat contained, given how it's being used and how
the people that are trying to develop this market are
intending to use it. They see it as a low-value
transaction to substitute for cash, a way to facilitate
and get people through lines, to add value for coffee
merchants or sporting events, et cetera. So in that
c context, I don't see a lot of significant issues with
respect to how companies have developed systems and
developed controls and applied the appropriate security
controls.
Where we may run into some issues is expanded beyond that, expanded beyond what was actually intended. And that's where government needs to be thoughtful in terms of, what are the signals that you want to send to the payments providers, what are the signals you want to send to the cell phone manufacturers and the device manufacturers, as well as what needs to be done to work together to solve these sorts of issues having to do with liability, which is a huge issue. And again, people in the financial services industry have a very large chip on their shoulder with regard to liability, because they typically bear it in terms of the losses that come through.

Increasingly, the customers are starting to bear it through identity theft, and that's where the government has really stepped in and the Federal Trade Commission, in particular, has played a major leadership role in saying, look, we've got to develop solutions to address the identity theft issue.

So I'm going to stop there, because there's been a lot of things discussed today that I think are very solid points, but that one issue that I was most concerned about was the point about innovation and that we need to be mindful that we get great benefits from the innovation, but we also need to be forward thinking.
in terms of how do we protect consumers as technologies are used in ways that we're not anticipating even today.

MR. COVINGTON: Thank you, John.

Dr. Tadayoshi Kohno is an Assistant Professor at the Department of Computer Science and Engineering here at the University of Washington.

Dr. Kohno.

DR. KOHNO: Thank you very much. As Dr. Covington said, yes, I'm an assistant professor here. I've actually been in the computer security and privacy industry for about ten years. For those of you who know the industry a little bit, I used to work with Bruce Schneider's company back when we only had basically four full-time cryptographers and that was it, and that's when I worked with them; also another company called Sigital (ph.), and while I was there, I ended up doing some consulting work with Visa and MasterCard and a whole bunch of other companies.

So that's where I started my career in computer security. Then I went to graduate school and got my Ph.D. in the area of cryptography, so how do you design protocols mathematically to provide certain levels of privacy or integrity, et cetera. And I also analyzed a whole large number of real systems both in the academic world and when I was a consultant, such as
voting machines and other types of RFIDs.

I should start off by saying that actually I really am not in the contactless payment space; I'm in the computer security and privacy space. And my research touches a little bit on contactless payment systems, but I kind of want to start off by talking about security and privacy in general.

And so the first question that I always try to ask my students or other people when we're talking about technology is, you know, raise your hand if you know exactly what security and privacy means for contactless payment systems.

So either everyone is being shy or people realize that we actually don't know what security and privacy means. I think that's one of the main issues that I'm very glad to see this type of forum and other types of forums address.

If we step back a little bit, one thing that we see is that often times in the media they portray security as this binary. You know, they say these cards we have are horribly broken; they're very insecure. Or they say that they're perfect. But in my view, security and privacy is not a binary. There's no such thing as perfect security. What we really need to be asking is, who are the parties involved in this particular type of
technology, what are their goals and what assets do they value, and does it provide an adequate level of privacy and security under these circumstances.

And many other people today are talking about this very complex ecosystem, and I think that's actually a very important point to keep in mind. If we take this approach that computer security and privacy is a binary, we might end up in a world where we just kind of dive into a bunker and say, you know, let's get rid of all technology and stop innovating.

On the other hand, if we take the other end of the spectrum and say there's no problems with this, we might end up innovating and taking technologies in new directions that actually end up putting us in a much worse scenario.

And I believe neither is right. Really, we need to step back and say again that security and privacy is not a binary; but what is this landscape, who are all the parties involved, what are their interests, and can we figure out a way to balance all these interests.

So I might say that there's really this seesaw between security and privacy and cost and usability and time to market, and we really want to figure out the right balance to the seesaw. And now
here's an opportunity to say, well, what is the right balance, what does this balance mean? And actually I don't know the answer to that, and I think it's great to see these type of forums where we get more and more people together to talk about this and try to figure out what is the right balance for contactless payment systems.

So one thing that I think I would -- let's see, trying to keep on track.

So I think towards getting to a point of figuring out what is the right balance, I think it's very important for everyone to be very open about how their systems work or what their requirements or criteria should be. And so for computer scientists, I think this means that we need to not just look at the technology but try to understand the business factors affecting the contactless payment systems. But at the same time, I think I would like to see the contactless payment industry being more open about exactly what protocols are they using, not necessarily relying on proprietary systems, because as we know from the past, proprietary systems have a tendency to have been broken, but to be more open about their processes and exactly how their systems work.

My second point that I wanted to make is that
there are many possible -- if we look at these
technologies, they're making possible ways of innovating
that we haven't thought of yet, and I would like to see
more interaction about what are the actual challenges
that people are facing and how can we innovate.

And so earlier today I saw lots of discussion
about how challenging it is to replace the back-end
systems. So we have this large deployment of these
point-of-sale readers, and the actual costs, I think
Dave Moorman talked about the actual costs to replace
these readers can be very expensive. And so the
question we have in our research group was, well, what
could we do to actually improve the security and privacy
of these contactless payment systems without actually
changing the back-end readers and without also changing
the usage model of these contactless payment cards.

And one approach we came up with was actually
kind of talked about by others before, but we actually
implemented it, was to take a passive RFID tag and put a
little bit of accelerometers or motion sensors on them,
and what we can now do is that we have can have this
passive RFID tag in our wallet and walk around, and if
anyone tries to read it, they will not actually be able
to read it. But as soon as we take it out and take our
wallet out and wave it or do a certain small pattern in
front of the reader, the contactless card itself will
get power from the reader and then will detect the
motion and say, am I doing the characteristic motion
that would allow me to communicate, and under these
circumstances and only these circumstances it would
actually transmit.

And so this is one potentially cheap way to
improve the privacy and security properties of these
contactless payment systems without actually changing
the back-end systems. So this is just one example of
one type of way of innovating. I suspect there might be
many other types of ways of doing that, but I want to
make sure we keep these in mind.

The other thing that Alissa talked about
earlier that really drives home to me was the point of
consumer education, and here's another opportunity where
technology might be able to help with this education. So
you could actually think about making some technology
that you would wear in your pocket or some other type
of, maybe wear on your wrist or wear on your belt that
would actually tell you when your RFID's are being read.
Or it could actually, you know, this little thing that
you have on you and if you get a new RFID -- if you go
to a store and they give you RFID tags, they'll tell
you, by the way, do you know you have these RFID tags
near you.

Other things that we might consider doing as a community is setting up public kiosks where, as a community service, some organization might set up kiosks, and then you walk by and they say, by the way, do you know you have these RFID tags, and I just read your names.

So like I said, my area is not actually in the contactless payment space. My area is computer security and privacy broadly. And I know I have five minutes left; I actually won't use it all.

My main points is that I would like to see more discussion about what does security and privacy actually mean in this space, and how can we come to some sort of middle ground that's in everyone's best interest. And again, several ways of doing this: One is, of course, computer scientists and computer security experts need to compromise and they need to say, well, we're not going to expect perfect security because perfect security doesn't exist; we need to understand what your threat models are so that we can come up with technologies that fit those threat models.

At the same time, I would like to see industry be more open. Again, I'm not in this industry so I apologize if I'm insulting someone because you
already are open, but I'm hoping you will be more open
and not use proprietary algorithms but tell us exactly
how your systems work so we don't get into confusing
scenarios where it's "he said, she said" and we don't
actually come to a consensus.

And lastly, I really do think there's great
opportunity to innovate, and by coming to a better
consensus about the practical constraints that the
industry is facing, whether it's back to maybe we can't
read or play back systems, et cetera, computer
scientists can then say, okay, well, under these
constraints, this may be how we can innovate a solution.

And so that's it.

MR. COVINGTON: Thank you, Dr. Kohno.

Paula Bruening is Deputy Executive Director
of the Center for Information Policy Leadership of
Hunton & Williams, LLP.

Paula.

MS. BRUENING: Thank you very much, and thank
you to the FTC for inviting me to be here today and for
giving us such a gorgeous day in Seattle.

There's always a challenge in being the last
person on the last panel, because in some ways you feel
like everything that you had planned to say has already
been said, but I do think that in being asked to talk
about transparency and consumer education, this really is not a bad place to sit, because it allows me to highlight some of the things that have already been said today and maybe expand upon others.

I think it's pretty clear, both from what we've heard today and for all of us who have been watching the evolution of this technology and its deployment over the last few years, that there is something about RFID technology that despite all the benefits that it may well offer us, it makes people uneasy.

It's an invisible technology. It's used in a way that's somewhat passive to the consumer, in some instances, where the consumer doesn't necessarily have to engage in its use, although that is not the case in contactless payment systems. But I think that it raises the specter of surreptitious surveillance and tracking in a way that other technologies, even though they may actually be functioning in similar ways, they don't raise that concern for consumers. And so I think this is an area where transparency and notice about the technology is really, really important.

And I think that in the case of RFID technology, you're talking about transparency and notice in two ways.
First, notification about the fact of the
technology itself is really important. You want to
build trust with your customer base, with consumers. If
you want deployment of this, you've got to be really,
really clear and honest and open about what is being
used.

And the second is notice and transparency
about any kinds of ways that this technology is being
used to facilitate data collection and data sharing and
use.

And when you talk about contactless payments
in closed systems, you really are talking about a
technology that's being used in a certain kind of way
with financial institutions, but I think today we've
heard about, you know, use of this kind of technology in
things like cell phones where you're looking at the
possibility of data sharing between different vendors to
allow different kinds of services to be offered, and so
you're talking about the privacy of data collection and
use, as well as the concern about RFID technology
itself.

I think there's been a lot of discussion
about notice over the last few years, about notice being
challenging, that perhaps consumers don't really
understand notices; they're difficult to write; it's
complicated; you can't make a consumer read the notice that you send. And I think there's some truth in many of those observations, but I think there still is a very important role for transparency in notice, and they remain fundamental to sound, responsible technology deployment and data collection.

And they really encourage an enhanced engagement by the consumer when you're talking about a technology that is somewhat silent and not so obvious. It also encourages disciplined data use and, obviously, as Katie said, it opens the company up to scrutiny about how the technology is being used, and it allows for regulation in a flexible and nuanced kind of way.

But I think overall it's important to think of it as a means to build trust with your consumer base, and also it's fundamental to the guidance that's been put out there about RFID deployment, much of that guidance which has been developed by companies and industry.

I think in the case of RFID, this can be particularly challenging because of the nature of the technology; and in many cases, RFID, when you look at different kinds of deployments, is out there in the environment; it's not necessarily something that you can put your hands on immediately.
But as I said before, in the case of contactless payments, I think this is the easy case. This is a closed system. This is a situation where there are many, many opportunities to engage with the consumer, to give them information: at the time that they apply for the card itself; when the card gets sent to them, there's an opportunity there; with the monthly statement. And the companies that deploy this are sophisticated companies that have Web sites that can inform consumers on an ongoing basis, because, as we know, this is an evolving technology; we're finding different applications and different ways that it can be used.

One proposal that has been out there, and I think that has been picked up by this industry, is to have some kind of a logo that immediately indicates to the consumer that there is this technology in place. I know that there are projects under consideration in Europe and within U.S. industry to put that kind of logo out there. I think that such a logo is a good idea, but I think that behind it there really needs to be additional information that gives the consumer more information about the benefits and the possible risks of the use of this technology and allows them to make better decisions about safeguarding their card and
making good decisions about where they leave it and
making sure that they take it with them when they get
out of the cab.

So when we talk about transparency, we're
talking about compliance with applicable laws in this
case, but also about establishment and compliance with
sound information practices. It's real a dual kind of
challenge when it comes to this kind of technology,
particularly when we are looking forward to a world
where data is going to be used among vendors that are
all coming together to make a service or an application
available to the consumer.

And I think in closing, I would just like to
say that, looking ahead, it's important to remember that
this is really, to my mind, the cutting edge of a world
that we're creating that is going to have a much more
ubiquitous deployment of RFID technology, not just for
contactless payment but for all kinds of uses that
engage the consumer both in active and in passive ways,
that we're creating environments where we're going to
have sensor-based and radio technology offering us all
kinds of benefits and also presenting us with lots of
different kinds of challenges, and it's going to be
really important that we take on this question of notice
and transparency and creating a consumer base that's
really active and engaged and understands what they're involved with and what they're using as we go forward and create this new world.

Thanks.

MR. COVINGTON: Thank you, Paula.

Questions? Bob? Bob, could you identify yourself and --

MR. CALAFF: (Inaudible.) It really may be too early to ask this question, but where do we go from here? I think we have shared a lot of good information and opinions, and do we focus on best practices next? Do we focus more -- a little more deeply on where the technology is headed? Other things? I mean, I throw that out just for consideration. Thank you.

MS. RATTE: You have actually set up an excellent bridge to Eileen Harrington, who is our Deputy Director of the Bureau of Consumer Protection; she'll be talking to us a little bit about next steps, any minute now.

MR. MACCARTHY: Mark McCarthy with Visa.

One quick comment on this whole question of standards and regulation. I think we're pretty comfortable with where the FTC is right now on this concept of reasonableness as a way to approach security issues. You're using your UDOP authority. Maybe it
would be a little better if you had explicit guidelines
to do stuff on safeguard rules as opposed to UDOP. But
the general idea that there should be a reasonable
standard makes a lot of sense.

Once you start to get below that and say,
well, maybe we should all have uniform and very concrete
standards that all of the payment systems should live up
to, or the way they're doing in Europe right now,
they're trying to have uniform standards for all RFID
applications, as if there's something in common between
supply chain and payment systems and health care and all
the other RFID applications. That's probably a mistake;
or if you're going to do it, it's going to be at such a
high level of abstraction it won't be concrete
information. So that's a comment on security practices.

Alissa had a great point on mobile payments
and mobile banking, which is actually in play right now
at the Reserve Bank of India, which is, we all want to
have a situation where bank customers can get the
underlying banking services that they want and need
regardless of the mobile carrier, so you don't have to
sort of shop around for a mobile carrier at the same
time you're looking for banking services, but it's kind
of tricky to get there. I mean, you may be able to cut
a deal with one mobile carrier first, and the ideal may
be to have a deal with everybody, but you don't want to have a requirement that says banks can't provide mobile banking services to anybody unless they're prepared to work with all carriers, because then one carrier who doesn't want to sign a deal would stop the whole process.

So it's not clear how you get to the goal, but it's a goal that we think makes a whole lot of sense, and if there's going to be some further conversation and discussion about that, it's something that I think we would like to participate in.

And the last comment is on Hannaford. I actually checked with my corporate relations people. That's a very delicate situation that we're in right there. We can't comment and don't comment on the compliance situation of anyone with PCI, but it's important to emphasize there's a difference between actually being in compliance and validating compliance. Very, very delicate situation.

MR. COVINGTON: All right. I'm afraid at this point, our time is up. I want to thank our panelists.

(Applause.)

MS. HARRINGTON: Well, that and each of the panels today have been -- that was and the others have
been just terrific.

I think this is a wonderful venue for a really important session. We at the FTC really believe in what our current Chairman Bill Kovacic talks about as public consultations. We have been doing these kinds of sessions for almost two decades. We hold gatherings like this, whether we call them workshops or town halls or hearings, to educate ourselves and consult with others in that process in the most public way, to say there are important issues here, we need to dig deep, we need your help to learn what it is that we need to know in order to do our job as well as we possibly can.

So this particular public consultation grows out of the Tech-ade hearings that the commission held in 2006, "Protecting Consumers in the Next Tech-ade," looking at technology issues that were likely to raise consumer protection implications and issues over the next decade. And contactless payments specifically, and RFID more broadly, is one area that we looked at Tech-ade and we think we need to keep looking at and keep drilling down on.

What happens next?

The next phase of the contactless payment RFID public consultation will continue on September 23rd, 2008, when the FTC joins with the Department of...
Commerce at a workshop on RFID technology that will be held in conjunction with a European commission Department of Commerce symposium that's going to be held in Washington. The September 23rd event will be a half-day event. It will be held back in Washington, as I said, not here in Seattle. It will be at the FTC's New Jersey Avenue Conference Center, and there will be more information up on our Web site very soon about this.

I can't tell you how pleased we are to be able to get out of Washington. You know, the weather there stinks; it's pretty good here. But more than that, there is just a richness about doing these consultations around the country and not always staying in Washington. Now, I know we have a lot of people here who schlepped all the way out from Washington or New York, but we've got people here who are from this part of the country, as well, and other parts of the country, and we think that that's very important, and we think that it's particularly important that we join with the academy when we can to do these consultations, and to that end, we are so grateful to the University of Washington, School of Law, and to Bill Covington for so generously joining with us and hosting us here today.

We also are so grateful to the staff who have
worked hard and will continue to work hard on this issue, and our team on the RFID issue cuts across time zones and includes Julie Mayer, Katie Harrington-McBride, and Katie Ratte, who really have been the key people on this issue at the FTC, one from Los Angeles -- one from our Los Angeles office, one from our Seattle office, and one from Washington, DC. So we thank them for their incredible work on this issue, now and always.

(Applause.)

MS. HARRINGTON: And also Chuck Harwood for his leadership here in the northwest region, for taking this issue on in the northwest regional office portfolio. The lead on this issue in the agency is right here in Seattle. We also want to thank others from the Seattle office who have helped out today: Charles Gust, Josh Kohls, Samantha Woo, Denise Pruitt, and David Goldfarb. Thanks to -- where are all of them? There are others. There they are. Thank you.

(Applause.)

MS. HARRINGTON: So thank you all for coming. I think this has been a rich session. I think we will continue inviting you to learn and discuss with us. These are important issues, and we always want to make sure that as we move forward, that we not act in a way
that is precipitous. We don't want to squelch innovation, but we also are very serious about using all of the tools that are available to us to protect consumers when consumers need protection.

And so we look forward to continuing to discuss these issues, and we'll see you in September in Washington, I hope. Thanks very much.

(Applause.)

MR. COVINGTON: We have one more announcement.

MS. MAYER: We have this facility courtesy of Bill Covington and the clinic and the law school, but we can't really host you, but we would love everyone who has made the trip, certainly, to join as many of us as possible for drinks at the Big Time Brewery; it's on the Ave, University Avenue, just one block west of here on 41st Street. So if you want to make the walk, it's a beautiful day, hope you can join us. Thanks.

And thank you all for coming, again, and participating.

(The proceedings adjourned at 4:57 p.m.)