

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

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		
2		
3	Welcoming Remarks	
4	William Covington, Moderator	3
5		
6	Introduction to Contactless Payment:	
7	What Is It and How It Is Used	
8	Katie Harrington-McBride, Moderator	11
9		
10	Consumer Understanding and Acceptance of	
11	Contactless Payment Technology	
12	Charles Harwood, Moderator	41
13		
14	Contactless Payment Cards	
15	Julie Mayer, Moderator	92
16		
17	Mobile Payment Devices	
18	Kathyrn Ratté, Moderator	172
19		
20	Meeting the Challenges: Strategies and Approaches	
21	William Covington, Moderator	219
22		
23		
24		
25		

1 Let me just share a few administrative details
2 with you before we get into the work of the day.

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

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

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

22 And last, but far from least, this building is
23 totally Wi-Fi'd, which is both a blessing and a curse to
24 those of us who are faculty. So for those of you who
25 wish to access the Internet, you can go to the

1 University of Washington website. The network ID is
2 Event 0217. That's Event 0217. Now, the challenging
3 part. The password is W8L2+B9N3+Q9M3. Now, I have a
4 number of papers at the place where I am sitting which
5 contains this information. So if you were unable to
6 keep up with this, I am more than glad to provide you
7 with the access information.

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

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

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

23 But then, secondly, I hope we can offer you
24 today an informative and useful program and that you'll
25 also have the opportunity to learn too. You'll have

1 something to learn from it, and hopefully you'll take
2 time to contribute to our program as well, and to ask
3 questions, comments, continue the dialogue during lunch.
4 Feel free to talk to any of us in the halls.

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

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

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

23 And the idea that somehow you can quickly and
24 easily pay for small transactions or maybe even large
25 transactions by just waving a device or even waving your

1 wallet in front of a reader or tapping a reader is a
2 concept that just sounds wonderful to consumers. It's
3 quicker, it's easier. Moreover, it might provide
4 opportunities for better recordkeeping as far as
5 consumers understand it. It might provide
6 opportunities -- it just simply has some amazing
7 opportunities or benefits.

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

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

24 We're also going to be talking about just some
25 of the ways in which that technology is being used now

1 and some of the ways in which it will be used in the
2 future.

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

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

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

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

24 So what we've been dealing with, even in the
25 past four years, is this rapidly changing and morphing

1 technology. And one of the things that we're hoping to
2 hear about more today is try to get a sense of where the
3 direction is, what directions these technologies are
4 going in, because that's important to us at the FTC. It
5 helps us get a better sense of what we need to
6 anticipate as a regulatory agency, as a consumer
7 protection agency and, frankly, as a consumer education
8 agency. A lot of our interest is simply in
9 communicating, educating consumers about their rights
10 and responsibilities.

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

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

21 So, in fact, today we're going to hear from
22 some folks who have already dealt with the use of
23 contactless payment, smart cards, whatever you want to
24 call them, in other countries. And that information
25 today, I think, will be useful to all of us. It gives

1 us a sense of how consumers will be using technology,
2 and will also help us understand what might happen here,
3 and it will also give us a sense of what some of the
4 international challenges are, some of the cross border
5 challenges are for us as we deal with these issues.

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

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

21 And with that, I think we're probably ready to
22 start our first panel. And I understand our first panel
23 is an Introduction to Contactless Payments and will be
24 moderated by Katie Harrington-McBride, and there she is
25 right there. Katie. Thank you.

1 **INTRODUCTION TO CONTACTLESS PAYMENT:**

2 **WHAT IT IS AND HOW IT IS USED**

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

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

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

25 We're going to have formal presentations.

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

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

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

25 And then to Randy's right, we have Dan

1 Littman, who is an economist at the Federal Reserve Bank
2 of Cleveland in their Payments Research Group. Dan is
3 going to provide us the bigger picture, the even bigger
4 picture on where contactless fits into the payment
5 system generally.

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

9 MR. VANDERHOOF: Thank you very much, Katie.

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

23 Our organization is made up of over 180 member
24 groups. They represent all of the industry,
25 participants in the payments field, as well as in the

1 identity and the security field. So we have a rich
2 community of knowledgeable people who understand the
3 technology, who understand the markets and who
4 understand the end users, which are either the
5 consumers, the retailers, the businesses, even our
6 Federal Government in terms of how they apply this
7 technology in their day-to-day lives.

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

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

20 Well, over time, we've seen different changes
21 being made to the payments infrastructure. We've
22 introduced other technologies than the plastic or
23 magstripe. One ever the really breakthroughs was the
24 Exxon Mobile Speedpass RF-enabled fob as a means to
25 deliver a payment system as the first real model in the

1 United States of having an alternative delivery system
2 to execute a credit or debit transaction.

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

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

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

25 The acquirer's role is how they interface at

1 the point of sale in gathering that credit card
2 information. Then it's identified by either its
3 branding of MasterCard, Visa, American Express,
4 Discover, Capital, and then routed out through the
5 network to the issuer who issued that individual's card.
6 It's then authenticated, sent back to the merchant
7 terminal with an authentication and the transaction is
8 completed. All this happens in milliseconds.

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

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

21 And, typically, those merchants have primarily
22 depended or used cash or checks for payment rather than
23 people pulling out their credit card. So the fast food
24 or convenience stores, the stadiums, vending machines,
25 movie theaters, taxi cabs, what they all have in common

1 is traditionally these have been heavily cash-oriented
2 merchant chains that are now, because of the speedy
3 convenience factor, are starting to open and to start to
4 use cards as a means of payment as well.

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

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

22 The last study we completed was in April of
23 2008, and we were able to compare that data with the
24 data we generated our initial study in 2006 to see what
25 kind of attitudes have changed. I think some impressive

1 information came out of that report.

2 9 percent of the population are contactless
3 payments users now, which is a significant increase of
4 where we were two years ago. People are more
5 knowledgeable now of what contactless payment is. So
6 they're beginning to understand it and make decisions
7 about whether it's right for them or not, but at least
8 they're now knowledgeable enough to make an informed
9 decision.

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

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

23 So we asked a lot of questions about -- both
24 from users of this technology and even people that
25 haven't used it yet what their perceptions were about

1 the safety of contactless payment.

2 68 percent of them said they thought that this
3 technology was as secure as their debit/credit card with
4 signature technology. The number of people who cited
5 that safety was their primary concern for not using it
6 actually has declined in the last two years. As people
7 become more informed about it, they're less -- we've
8 answered a lot of their questions.

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

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

24 So I think the important take-away there is
25 that we're never going to have a consumer population

1 that's totally comfortable and feeling safe and secure
2 about payments, but this technology doesn't raise any
3 significant higher barriers to that concern than any of
4 the other existing products that are on the market.

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

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

22 And without going through all of the bullets
23 there, the highlight for a consumer is, I just want to
24 be able to trust my payment product. I want it to be
25 fast and easy and simple. And if you can make my life

1 simpler or get me through the lines faster and also
2 allow me to do that transaction and feel safe, then I'm
3 certainly going to be attracted to that.

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

15 And the retailers, which are the ones that
16 have to invest in the infrastructure to accept
17 contactless payments, rather than trying to drive this
18 through the entire retail chain, what the brands did and
19 the issuers did, which I thought was very bright, is
20 they looked at the target market which would achieve the
21 highest benefit, which was the convenience stores, the
22 fast food locations, et cetera, because they were going
23 to be the folks that would prove whether or not this new
24 payment platform was really to going to catch on in the
25 consumer market.

1 So when we reached out to the consumer -- to
2 the convenience stores, the fast food chains, the movie
3 theaters and such, what they found was that, yeah, not
4 only did this move people through their lines faster,
5 but it also created a better shopping experience for
6 their consumers and, therefore, the consumers started to
7 populate those stores more frequently. They started to
8 use the card in more creative ways and add additional
9 purchases. All of this was a way where retailers could
10 get more traffic through their lines and be able to
11 target some more benefits to their consumers.

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

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

25 Because this is simply a closed payment

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

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

17 Taxi cabs -- the number of cities -- I live
18 just outside of Philadelphia. Philadelphia is one of
19 the first cities to implement payment with a credit card
20 at a taxi. What a great idea. I mean, how many of us
21 have been riding in taxis and scrambling for money
22 because we didn't have an option of using the card in
23 our wallet. This has been -- you know, consumers love
24 this idea. Taxi drivers aren't so keen on it for other
25 reasons.

1 There was a pilot with the Ohio Turnpike to
2 use this as a means of payment on the highway. They
3 couldn't accept credit cards at a machine on the highway
4 because, again, the outdoor infrastructure and place and
5 the risks associated with the swipe not being able to be
6 read, the slowness of the transaction, having to sign it
7 and things. But now having this contactless card or key
8 fob device, they can achieve their speed of transaction
9 and reliability of transactions, and it opens up another
10 means of convenience of payment that motorists didn't
11 have available to them before this technology came on
12 board.

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

24 What New York City is piloting is by
25 implementing contactless payment at the turnstile.

1 They're going to bypass that whole line. When people
2 enter the system, rather than going to the kiosk or
3 going to the booth, transferring their payment to a
4 transit pass or transit card, they can now walk right to
5 the turnstile, tap their keychain device or their phone
6 or their card, and it will deduct only the fare for that
7 transaction and they go through the system. So opening
8 up that opportunity, consumers are going to like that.
9 Certainly, the transit operators feel very comfortable
10 as well. So this is the kind of innovation that is
11 spurring with this capability.

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

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

24 Nobody questions the fact that cash is still
25 the most widely-used method of payment, and there's no

1 security associated with cash. If I lose my wallet or
2 if I lose the cash out of my pocket, you can't identify
3 it. So the advantage is it's anonymous. The
4 disadvantage is that there's no way to tie it to the
5 individual.

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

19 So radio frequency is probably the key point
20 that we tend to circulate back to. This is different
21 because we've never had a payment product that generated
22 our account information through a radio frequency
23 interface to the terminal. It's always been a
24 deliberate act of a user swiping their card through a
25 terminal or entering their account number through their

1 keyboard, and now we're doing this airwave
2 communication.

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

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

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

24 Even if somebody would introduce a reader
25 device that's more powerful with a greater read range,

1 the amount of range that is increased by that
2 significantly deteriorates the information that is
3 transferred between the card and the reader.

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

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

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

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

25 If you're a reader and want to understand a

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

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

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

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

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

25 And, you know, we're going through a period

1 now in the world, especially in the developed world, and
2 the United States being part of that, where there's more
3 payments innovation than there ever has been before.
4 And, of course, that's all caused by the information
5 revolution and computer technology. It's not caused by
6 anything that's unique to the payment system. And
7 contactless cards are just one of those innovations and
8 probably not the most important of those innovations in
9 terms of the current time.

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

22 Randy mentioned top of wallet, the goal of all
23 these payment innovations, particularly the ones that
24 are carried around people's pockets or purses is to get
25 to top of wallet. And contactless is very far from

1 being top of wallet. It's not even top of wallet
2 probably in Hong Kong or Tokyo or London. Maybe for
3 some people, but certainly not for the masses.

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

12 So probably we have somewhere in the area of
13 200 billion transactions in the U.S. that are in the
14 retail space, and roughly half of those are cash still.
15 But nobody really knows how many cash transactions there
16 are. It could be 80 billion, it could 120 billion;
17 we're not quite sure. The rest of them we have a pretty
18 good idea.

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

1 traditional payment vehicles.

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

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

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

21 The payment system is something that evolves.
22 It's not something that has revolution that occurs in
23 it. And so contactless or any of these other
24 innovations, they're all based on all the previous
25 innovations that occurred before them. And, you know,

1 contactless is something that grew out of cards and
2 which grew out of other payment technologies, and so
3 it's not something that just is in its own silo. It
4 sits on top of all the other payment technologies that
5 exist.

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

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

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

25 And, of course, it aspires to be dominant or

1 at least present in every market. And over the next 10
2 years, it will. In the next 10 or 15 years, it may do
3 through a mobile form factor as opposed through FOBs or
4 the other form factors that are available.

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

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

19 Why does the Fed care about this? Sometimes I
20 wonder too. So, you know, the Fed, don't we run the
21 declining part of the payment system? We do. But it's
22 still a huge part of the payment system. Still there's
23 about 30 percent -- we process about 30 percent of the
24 checks, and checks still represent 30 percent of all the
25 payments that are not made in cash, but declining.

1 So why are we concerned? And I'm speaking for
2 Dan, not the Federal Reserve. We're concerned because
3 as a central bank, we're interested in the efficiency of
4 the payment system. We're interested in access to the
5 payment system, and we're interested in the risk of the
6 payment system. So in terms of efficiency, all payment
7 systems create friction. You know, you have to keep the
8 economy lubricated in some fashion, and the payment
9 system is one of the things that does that.

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

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

24 So contactless is something that creates more
25 efficiency in the payment system, and Randy has talked

1 about that a little bit, in terms of the speed of buying
2 hamburgers at McDonalds or whatever or buying gasoline.

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

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

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

23 How much we do it in the United States as
24 opposed to in South Africa -- it's going to have more
25 impact in South Africa or Kenya than it is on the U.S.,

1 but it could bring some people into the formal payment
2 system that are not today there.

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

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

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

22 But, you know, we are interested in consumer
23 risk, and along with the FTC, we're one of the
24 regulators of consumers through -- or consumer rules
25 through the Regulation E. And there we are here or I'm

1 here to try to learn more about what other people think
2 about risks in this area.

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

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

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

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

20 MR. LITTMAN: I guess I wouldn't weigh them on
21 a scale like that. The one thing I would say is that
22 people are not aware of the risk aspects of the dominant
23 payment vehicles. Just like on anything, we focus on
24 the new types of vehicles, whether it's Obo-Pay or
25 contactless payments or PayPal. We focus on those

1 because they're new and novel, but we don't focus on all
2 the risks -- characteristics of check clearing.

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

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

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

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

25 MR. LITTMAN: You know, I know that they have

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

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

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

20 (Recess taken.)

21
22
23
24
25

1 **CONSUMER UNDERSTANDING AND ACCEPTANCE**
2 **OF CONTACTLESS PAYMENT TECHNOLOGY**

3 MR. HARWOOD: So this is the next panel in our
4 program today, and it's entitled, Consumer Understanding
5 and Acceptance of Contactless Payment Technology.

6 And as with the previous panel, our plan is to
7 have each individual provide their -- each panel provide
8 their presentation, and then we'll take questions at the
9 end of the presentations. I may intervene with one or
10 two questions, but for the most part, we'll wait until
11 the end to take all questions.

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

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

25 MS. GOLINSKY: I also want to thank Julie

1 Mayer and everyone from the FTC for organizing this
2 conference. I applaud you for bringing us all together
3 to talk about this issue, which is important to
4 consumers and, of course, is important to MasterCard as
5 well.

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

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

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

22 And I am also going to then touch on the two
23 issues that seems that most consumers bring up or
24 consumer groups, which is the points about security and
25 privacy, just to reiterate some of the points that were

1 already made on the last panel about what the security
2 features are on these cards and sort of how they work.

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

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

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

24 And I mention that only because certain
25 questions you might have about what's done or what

1 communications are made, MasterCard really works hard to
2 educate consumers about PayPass, but so do our issuers
3 who are the ones who are actually issuing you those
4 cards that have that functionality.

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

8 (The video was played.)

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

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

23 There are 24 countries right now where
24 deployments or consumer trials are taking place, and we
25 now have acceptance outreach of 109,000 merchant

1 locations.

2 So you can see that this is something that is
3 taking off, and I think that's sort of the theme of
4 today. This is a technology that's really on the move,
5 and it's starting to rise. And what do consumers think
6 about it?

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

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

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

23 What does MasterCard do to give consumers a
24 little bit more information about these cards? And I
25 was talking to Jennifer earlier today about her studies,

1 and she did some studies a year ago and I know she's
2 going to start doing some additional ones. I think what
3 we're seeing as we see a greater take-up of this
4 technology and interest in this kind of payment is that
5 we are reaching out more to consumers, us and our
6 issuers, to make that they understand what it is.

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

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

22 Another important key piece about this is the
23 zero liability piece. MasterCard offers zero liability
24 on all its payment cards, PayPass enabled or otherwise.
25 So that is a huge consumer security feature -- it's not

1 a security feature. It's a feature that gives you piece
2 of mind that if for some reason there is anything
3 fraudulent going on with your card or unauthorized
4 purchases, you have the luxury of zero liability on all
5 your PayPass enabled cards.

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

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

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

25 So what we're seeing is that consumers really

1 like this. They like the efficiency. They like the
2 speed. They like the convenience, and it's targeted to
3 places where speed and convenience are important. And,
4 of course, MasterCard is going to continue to test and
5 monitor, as well as our issuers in doing that.

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

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

19 Now, of course, the PayPass enabled card is
20 different because it has this chip technology and you
21 have the radio frequency. So MasterCard has a number of
22 security features in place to try to address that. And
23 one of the things that I can mention is that we now
24 mandate that the cardholder name cannot be embedded into a
25 chip on a PayPass enabled card.

1 In a lot of the research papers I read and
2 comments posted, there was concern about the privacy
3 piece that your name somehow is getting out there.
4 Somebody could, if they were able to get a reader, could
5 read personal information about you. That's not the
6 case because MasterCard now mandates that the cardholder
7 name cannot be embedded in the chip.

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

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

25 I was going to say some more, but I know that

1 my time is up. So I will pass to Jennifer, and I'm
2 happy to take questions at the end.

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

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

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

19 MR. HARWOOD: Thank you for clarification.
20 Our next speaker is Jennifer King. Jennifer is with the
21 Samuelson Law, Technology and Public Policy Clinic at UC
22 Berkeley School of Law, and, again, you'll find
23 Jennifer's more complete bio in our materials.

24 Jennifer is going to talk about a study she's
25 currently engaged in that is directly on point with the

1 grander interest in consumer acceptance and
2 understanding with regard to contactless payment
3 technology.

4 And I think you have a Power Point?

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

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

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

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

1 with their every-day environment.

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

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

18 And so we investigated something we call
19 mental models, which I'll explain more in a minute. And
20 we are looking at how people understood radio frequency
21 in general and how they understood RFID specifically.
22 And so these findings are, again, preliminary because we
23 started with a very small sample, nine subjects. We put
24 it out there at this point because we wanted to get
25 feedback on how we designed it to see what we wanted to

1 do for the next round of testing.

2 And so we focused on trying to find three
3 novice users; people who had no concept of what RFID
4 was, three intermediates; people who had heard of the
5 concept but couldn't necessarily articulate what it was
6 and how it worked, and three experts; people who really
7 did actually understand what it is and how it worked,
8 and so, again, with the transit cards, credit cards and
9 the ePassport.

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

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

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

1 object that we were testing worked specifically.

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

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

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

25 So we looked at -- we talked to a handful of

1 UC Berkeley graduate students, some staff members, as
2 well as some members of the public. About half of them
3 were technical and half were not.

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

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

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

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

25 Credit cards we actually found that over half

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

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

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

17 And so the structure of that interaction, the
18 idea that you can just walk through the turnstile, have
19 it read the card, they get some kind of visual feedback
20 or a beep that it's actually been read, the fact they
21 don't have to wait in line, that all really made sense
22 to people with regards to transit. It had really
23 obvious benefits and efficiencies for people who didn't
24 have to wait in line. They didn't have to deal with
25 paper tickets. And just like the D.C. Metro where it

1 uses these paper tickets, generally that if you get them
2 wet, they just fall apart and they stop working. So the
3 idea of a plastic card really made sense to people.

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

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

18 Many of them were very concerned about the
19 security of the entire system. Identity theft was
20 mentioned quite often in our talks. And financial data
21 was seen as something far more personal to them. They
22 had much more of a personal impact if something was
23 compromised. And, interestingly, most people actually
24 said they wanted what they called the security of
25 signing for a purchase.

1 A few people had already experienced the new
2 change, which I think it's either under 15 or under \$10
3 or maybe it's under \$25 transactions where you no longer
4 necessarily have to sign. Most of them were very
5 concerned about the fact that they didn't have to sign
6 anymore. It didn't cognitively make sense to them, even
7 though I don't think those signatures in general really
8 mean anything. My colleagues in the credit card
9 industry can probably clarify that, but I think it's
10 kind of a false sense of security is my understanding.
11 But for our users, it really did mean something.

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

18 And then, finally, the Passport. This was
19 the one where, in particular, people really didn't feel
20 like they had any benefits. Obviously, this is not a
21 payment system, so not as relevant for our discussion
22 today. But just, in general, people didn't see that
23 they had any personal benefit from the fact that RF
24 technology was included in the Passport. They really
25 thought it was only going to benefit the government, and

1 they especially didn't see why it needed to be remotely
2 readable. It just didn't make sense to them.

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

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

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

24 And so the commonalities that we found across
25 all these three objects was this notion of convenience

1 and efficiency, which you've already heard several times
2 today. Certainly, that's, I think, a benefit the
3 industry is talking about, and it is one that consumers
4 are seeing as well.

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

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

21 And then the context is really important,
22 which I think is an important take-away for today, which
23 is whether or not the use that you're trying to put
24 forward really aligns with how people expect it to work.
25 And, you know, we were left with the question after

1 doing this is if we thought the issuers had more
2 benefits with using this than the actual users.

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

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

20 I'll go ahead and stop it there.

21 MR. HARWOOD: Jennifer, I have one quick
22 question for you, and it's stated in your summary of
23 your written materials. You talk about the fact that
24 depending on the type of form factor that's being used,
25 that changes the level of consumer understanding. Did I

1 read that correctly? For example, it appears that in a
2 cell phone, which consumers are already commonly used to
3 using, that's more confusing for them potentially than
4 it appears than if something is a kind of new form
5 factor they're not familiar with in terms of their
6 understanding of how the system works or what their
7 concerns should be about --

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

16 But today, it's -- well, A, it's difficult to
17 even get a phone now without a camera in it. This is
18 actually something we studied at Berkeley, where we
19 found that people really adapted to the inclusion of the
20 camera, and they use it in ways that -- when you thought
21 about photography 15 years ago, you would have never
22 thought that you'd take a little tiny 640 X480 picture
23 of something and it would be of any use. But, instead,
24 we find that there's actually really good uses for using
25 cameras in phones.

1 I would expect integrating payment into phones
2 is going to be very similar. I mean, you'll have people
3 who will just -- there's a good study done by Nokia
4 actually where they were testing out Nokia NFC phones.
5 And they had a poster they put up with either a 2D bar
6 code or an RFID tag on it, and they basically walked
7 around, I think, Helsinki asking people to figure out
8 what to do with the phone and the poster.

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

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

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

24 MR. HARWOOD: Thank you, Jennifer.

25 So our next speaker is Jean Ann Fox. Jean Ann

1 is the Director of Financial Services for the Consumer
2 Federation of America, an NGO or a non-profit
3 association with more than 300 consumer groups around
4 the United States.

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

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

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

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

19 And I'd like for you to just bear in mind that
20 some of the selling points for the contactless payments
21 and the convenience of just tapping a card or tapping
22 your phone to make a payment is -- this is likely to
23 encourage consumers who have trouble making ends meet to
24 spend more money than they would have if they pulled
25 cash out of their pocket. That's one of the selling

1 points; that it increases the size of an individual
2 purchase, that you're not constrained by how much you
3 have on you.

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

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

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

23 If you're paying with cash, there's just not a
24 trail of where you spent your money and how much you
25 spent. Once you get people into using plastic or their

1 cell phone or whatever the next whiz-bang application is
2 going to be for contactless payment, now you create a
3 record and a paper trail -- not a paper, an electronic
4 trail of where money was spent, how much was spent.

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

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

16 And the information that's stored on your cell
17 phone with your passwords and a lot of personal
18 information -- people use their PDAs almost as their
19 computer in their pocket. All of that information is
20 going to be available, and the protections that go with
21 the security aspects of contactless payment are going to
22 be extremely important. This adds location information.
23 Not only how much did she spend and where did she spend
24 it, where is she at the time that that transaction is
25 taking place?

1 This can be used for profiling. It can be
2 used for proximity marketing. There was the movie where
3 the guy walks through the store, and the ads come up and
4 say, Jennifer, I see you have on a --

5 MS. KING: Minority Report.

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

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

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

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

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

25 MS. FOX: Was that the elephant's card or was

1 that sick guy's card?

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

4 MS. FOX: Inquiring minds want to know.

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

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

25 There are protections that go with using a

1 debit card that pulls money out of an account in your
2 name at the bank. They're not as good as the
3 protections for credit cards, but there are rules there.

4 But as we've been told this morning, you can
5 use contactless payment with stored value cards. Those
6 are gift cards, payroll cards, general spend debit
7 cards, the kind of cards that are being sold to unbanked
8 consumers to load their paycheck on it at Wal-Mart or at
9 check cashing outlets or other non-bank financial
10 service providers. And these cards can hold
11 considerable family resources.

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

22 So the deployment of contactless payment and
23 the new forms of it that are going to come shine a
24 bright spotlight on the fact that we need to have
25 uniformed, consistent, high-level protections for all

1 forms of payment so that consumers don't have to scratch
2 their head and say, is this card that's plastic and has
3 a MasterCard or Visa logo on it, you know, am I covered
4 by Truth in Lending? Am I covered by Electronic Funds
5 Transfer Act? Am I covered by the Fed's rules on
6 payroll cards? Am I not covered by anything? Should I
7 feel safe in using this card?

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

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

21 And I think that the fast pickup and the
22 comfort people feel with these cards is a direct result
23 of federal consumer protections, and we must upgrade
24 them for all forms of consumer payment so that the new
25 forms of payment are safe for consumers, there are clear

1 protections against an unauthorized use, there's a
2 dispute process, you can charge back an unsatisfactory
3 transaction.

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

9 MR. HARWOOD: Jean --

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

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

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

14 MR. HARWOOD: You can have ten seconds.

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

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

22 And MasterCard's zero liability doesn't apply
23 if you've had more than two unauthorized transactions in
24 a year. So somebody, you know, has skimmed your numbers
25 and has been putting charges on your card or taking

1 money off your card. If that's happen more than twice,
2 does the liability limit apply?

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

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

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

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

23 MS. FOX: No, this is different. And take the
24 example of the Scandinavian countries, where they're now
25 making payday loans using somebody else's cell phone.

1 They're called a short message service loans. So the
2 young folks are out partying on a Friday night and run
3 short of money. They text their request for a cash
4 infusion, which gets loaded on their debit card. They
5 pay 800 percent interest, and you've got to pay it all
6 back in two weeks. I don't know whether you could do
7 that without this new technology exactly that way. So I
8 think that there are some new wrinkles in the wine
9 bottle, and we will leave it up to our other speakers to
10 elaborate on those, but I think this is a new thing.

11 MR. HARWOOD: Okay. Thank you.

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

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

17 MR. MACCARTHY: I caught the word brief.
18 Thank you very much. I'm glad to be here, and I thank
19 you for coming all the way up here to listen to our
20 discussions. And our host, thank you for having us
21 here, and Julie and the Katies who put everything
22 together, thank you all. I think this is a great show.

23 And I'd like to thank especially my son,
24 Collin, who is on the sort of victory lap with me here.
25 He just graduated from high school, and we're out here

1 in Seattle and San Francisco to sort of have a little
2 vacation together, and I'm glad he came to watch me do
3 the show. He's a little nervous about all the lawyers
4 in the room. I told him that he should also be nervous
5 by the economists. They're also a threat to the common
6 man.

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

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

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

24 The key thing that consumers have to know
25 about this -- and this is why I'm pretty interested in

1 some of the things that Jennifer has found out about
2 what consumers are thinking, even though the sample size
3 is small. The key thing they have to learn is how to
4 hold the card. Really, do I point that thing? What do
5 I do with this thing? And so one of the key messages we
6 have to get to people is how you hold the card in order
7 to make it work.

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

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

18 Some of our numbers -- partially in response
19 to Jean Ann's point about people going broke using their
20 contactless card, three-quarters of our transactions are
21 under \$25. The places where people use these cards tend
22 to be places where it's low value, not high volume, not
23 high-value transactions. There is an increase in the
24 number of transactions. You can see the numbers there,
25 and there is an increase in the ticket size.

1 So those are the points that make it valuable
2 for the merchant to use the program, and it's for that
3 reason that we're seeing top merchant acceptance in the
4 United States growing pretty dramatically. Here are the
5 companies that we're working with and that have been
6 picking up the contactless card at the point of sale.

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

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

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

1 partly just to inform them how to use the card.

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

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

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

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

1 together to put in place something that protects all
2 consumers across the board. All right. That's our
3 consumer communications.

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

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

20 Risk assessment. There's a little bit time
21 here, I think, to pause and give you a little context
22 here. We do risk assessment all the time. It's one of
23 our major things that we do in our business, and we do
24 this for a very good regulatory reason and a very good
25 business reason.

1 The regulatory reason -- I think, Jean Ann
2 made reference to this -- is that for reasons that were
3 good and sufficient to the United States Congress back
4 in the '70s, essentially a public policy decision was
5 made to put the risk of unauthorized transactions not on
6 the cardholder. I mean, there are details of about \$50
7 and debit versus credit. But the fundamental decision
8 was made somebody in the payment system has to eat the
9 unauthorized losses. Fraud doesn't get put on the back
10 of the cardholder.

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

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

20 The second reason, of course, is if there's
21 too much fraud in the system, then people lose trust in
22 it. It's not a trusted, secure operation. People say,
23 I've given you information and what have you done with
24 it? You haven't protected it, and I'm not going to use
25 your system. So we've got enormously good business

1 reasons to try to figure out how to do this kind of
2 stuff right. That's in general.

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

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

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

25 Jodi made reference to what she called Dynamic

1 Card Verification value. We have a similar program in
2 place to protect information that's part of a
3 contactless transaction. But to understand it, you have
4 to go back a little bit, and this is what's going to
5 take me the extra minute.

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

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

23 The new thing that's part of our contactless
24 authorization is that that number changes with every
25 single transaction. So if you do get the number through

1 one of these hacks, you can't use it again for a
2 different contactless transaction. That's the magic.
3 We made that number change with every single
4 transaction. We think that addresses a large number of
5 the security issues.

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

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

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

25 The new specification that we're putting

1 together will require that the readers will first send
2 to the card an unpredictable number, which will then be
3 used together with the information on the card to
4 generate a dynamic number that will change with every
5 single transaction.

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

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

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

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

1 dealing with.

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

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

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

24 MS. GOLINSKY: I'd just like to make a comment
25 about zero liability. You know, MasterCard takes the

1 same view that Visa does. You know, one of the things
2 that becomes very confusing -- and I'm actually a
3 regulatory attorney and I get confused between Reg E and
4 Reg B and what they have and what they don't, which is
5 why MasterCard has a zero liability policy.

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

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

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

24 MR. HARWOOD: So let me see if we have some
25 questions in the audience. We have one right over here.

1 We'll start Susan Grant. We have time for about three
2 questions probably.

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

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

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

23 Most merchants, if they're worried about fraud
24 in their context -- and they should, because the
25 responsibility for fraud is theirs. The liability for

1 online fraud rests with the merchant. So they have got
2 every incentive to do this right. We've given them
3 tools to help out; one of which is the Card Verification
4 Value 2 on the back of the card. Merchants who ask for
5 that would be fully protected in this context.

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

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

20 It's verified by Visa, which is a program
21 we're offering for the merchants, where if they do it
22 and they put it in place, there's no way that the
23 cardholder information that was compromised in a
24 contactless transaction could be used to get that
25 information.

1 And we think some of the merchants are really
2 stepping up to try to take their own measures to protect
3 fraud in this area. I mean, many of them use, you know,
4 their own fraud screens like finding IP addresses that
5 are suspect IP addresses, and they'll decline the
6 transaction even in the context where the issuing bank
7 would approve it.

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

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

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

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

25 MR. HARWOOD: Samantha, we've got someone back

1 there? Great. Next question.

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

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

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

24 MR. HARWOOD: All right. One final question.
25 We'll go back there. Sorry about that.

1 MR. KOSCHER: Carl Koscher. So one thing that
2 I've been wondering about is one of the nice things
3 about the contactless cards is you can keep it in your
4 wallet and still tap it against the reader and it will
5 work. So I'm wondering once issuers start sending us
6 cards and we have a wallet full of cards with these
7 PayPass features on it, what happens then? Does one of
8 the cards get randomly chosen? Are consumers being
9 informed about that?

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

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

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

20 MS. REDFORD: Leann Redford with Visa. So
21 what you're saying is if you have multiple cards, how do
22 you pick the one at the point of sale, because it has to
23 be awfully close? So you're the lucky consumer, you're
24 holding a whole handful of -- you might say a whole deck
25 of cards in your hand, and you hold them towards the

1 reader. Our technology specifications say the reader
2 can't choose. We know what card we'd like you to
3 choose, but the reader doesn't get to choose for the
4 consumer. So the terminal says, whoa, I've got more
5 than one card in the field, please stop and have the
6 consumer choose which card they choose to pay with,
7 debit, credit, brand, whatever. Does that make sense?
8 We could technically solve that problem in our favor,
9 but that's not part of consumer choice.

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

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

20 (Recess taken.)

21

22

23

24

25

CONTACTLESS PAYMENT CARDS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

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

1 organization, who unfortunately was unable to come at
2 the last minute.

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

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

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

25 Part of that strategy are payment cards;

1 they've become a very crucial part in our lifestyle.
2 People use both types of cards for -- all three kinds of
3 cards for their payment needs, and they've really become
4 a great aid in terms of conducting transactions.

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

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

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

25 And lastly, I think, there are benefits to

1 having a card, in terms of chargeback feature, extended
2 warranty, and other value-added services that we add.

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

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

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

1 demagnetized.

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

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

22 So getting into customer communications, I
23 think a lot of people have talked about customer
24 communications and what are issuers doing to communicate
25 with their customers that they indeed have a contactless

1 card in their pocket.

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

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

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

24 So that's information there. In addition, we
25 have to include all of our other pieces of information,

1 keeping your information safe, and our card disclosures.
2 But at the end of the day, there's a lot of information
3 in this package, and it does tell the customer, yes, you
4 have a contactless card; and that's great, but the one
5 thing to keep in mind is, in our studies, only ten
6 percent of the people read the stuff in the envelope.

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

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

21 So the concern is, if I send out a bunch of
22 cards in the mail, and, here, I'll just put this back
23 into the envelope, and somebody in the mail stream
24 decides, hey, I'm going to read a bunch of cards today,
25 well, this is an actual contactless reader. I've waving

1 the card all over it. It's not reading; it's not
2 beeping. And just to prove that again, I'll go ahead
3 and -- (Demonstrating). It's not reading. It's to
4 protect our customer.

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

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

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

25 Anyway, but getting back to the point here

1 is, we are protecting our customers, and we are
2 protecting our customers in many different ways, and the
3 card is a secure card. When you look at how someone
4 could steal this information, and the one thing that we
5 have to think about is, when you steal information,
6 that's one thing, but what can you do with the
7 information you have is a whole other case.

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

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

25 So then you say, okay, well, then, I'm going

1 to make a bunch of fraudulent transactions on the
2 Internet. And as pointed out earlier as well, that can
3 be done; however, many consumers are -- or many
4 merchants are actually starting to use CVC2, which
5 basically is this three-digit number on the back of your
6 card, right? You can't read that wirelessly. It's not
7 on the chip.

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

17 So getting back to talking about security, I
18 did read a lot of the comments in the comments section,
19 and one of the things I did notice was a lot of people
20 were saying we should have more security around these
21 cards. And I would say, yes, that does make a lot of
22 sense; however, we also have to think about the fact
23 that we are working within an ecosystem, and this
24 ecosystem includes merchants and it includes issuers and
25 it includes consumers.

1 The more difficult you make something -- or
2 the more secure you make it, usually it means more
3 expense from the merchant's point of view, because
4 you're adding additional security features that cost the
5 merchants in incremental cost, it costs the issuer
6 something, and at the end of the day it also costs the
7 customer something, because they have to learn how to
8 use the card.

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

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

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

24 The first one is basically no security,
25 always on, so I just walk up and I tap the phone, it

1 will read -- it is reading, actually; it's just not
2 beeping for me.

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

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

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

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

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

25 MS. MAYER: I have one question for you

1 before you sit down -- or you can sit down.

2 MR. HO: Thank you.

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

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

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

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

25 MS. MAYER: Thank you for that tip.

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

9 Take it away, Dan.

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

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

23 A little bit about Tully's. We were founded
24 in 1992 by Tom Tully O'Keefe. If you're not familiar
25 with our brand, we are a custom, hand-roasted coffee

1 company. We do everything by hand; we don't use
2 machines; we have people up there sniffing coffee and
3 abstain from technology on that side of it as much as we
4 can, but also from a retail perspective, we obviously
5 embrace it as we need to do business.

6 We have 150 retail locations domestically.
7 Of those, 90 or so are corporate locations which are
8 using contactless payments. The others are franchise
9 locations. Additionally, in Japan, we have over 250
10 franchise locations. We just started up a company in
11 Singapore to open coffee shops up there. In addition to
12 the retail, we also have grocery stores; we're in over
13 4,000 grocery stores across the West Coast.

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

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

24 The first is quality. You have to have a
25 good quality product, which we believe we have. We

1 wouldn't be in business if we didn't have a quality
2 product.

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

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

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

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

24 So really from a convenience perspective, we
25 kind of started looking at the contactless, saying, is

1 it something that we can use to speed up our line? Will
2 people who have contactless cards not order the
3 super-double-tall-nonfat-soy-chai-latte-no-whip and not
4 hold up the line trying to figure out what they want to
5 drink?

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

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

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

22 Also, it's an option for our consumers. We
23 found some consumers have come up to us and said, hey, I
24 have this great, nifty tool; can I use it at your store?
25 And although that itself isn't necessarily a driver, I

1 don't think we're turning away customers when they come
2 up to us and say, oh, I'm not going to use your shop
3 because you don't have it. It is another option for
4 people that are very passionate about that and who do
5 want to use it.

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

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

23 So we did a pilot in five locations, and that
24 worked out very well. We use a Verifone Omni 3750, and
25 actually the ViVOtech reader that you see in front of us

1 here. Installation was pretty quick. It was pretty
2 cheap. And from a point-of-presence perspective, it
3 does kind of stick out in front of the register, and we
4 got a lot of questions when we first put them in saying,
5 hey, that's great; how do I use it? I can't tell you
6 the number of people that don't have contactless cards
7 that try and use that reader. It's a constant problem.
8 But that's neither here nor there, and I'll actually get
9 to that here in a little bit.

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

19 And getting to the results section, first of
20 all, I have to put a little PCI disclaimer, which says
21 that we don't save credit card numbers. Tully's does
22 not save any of that. We know the banks do. We don't
23 have access to that, so I have truncated data. So I've
24 got a bunch of numbers that have the last four digits,
25 and trying to figure out frequency, recurrence of

1 consumers. So it's not accurate, I can tell you that,
2 it's not 100 percent accurate, but it should be ballpark
3 in terms of what we're seeing in terms of repeat
4 customers, who's using it, and why they're using it.

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

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

20 Overall, as a percentage of credit card
21 customers that are using contactless, it is very, very
22 small still. It is a very, very small number of people
23 that are using contactless cards as opposed to regular
24 magstripe cards. And part of it is the saturation of
25 the cards out there. A lot of it could be, again,

1 different rewards that people have on cards that they
2 haven't been offered as contactless yet, but we're
3 expecting that to grow, but it is very small right now.

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

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

21 As it is now, it's not a big home run. It's
22 nothing that is going to significantly drive our
23 business currently, but also I would expect that to
24 incrementally change as we get more people out there
25 having these cards, as there's a greater education about

1 these cards, and as we put on additional, maybe,
2 marketing aspects of that to get people to come in.

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

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

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

24 MR. JOHNSON: Yeah, it definitely is. I've
25 got to say, you know, MasterCard, Visa, and AmEx have

1 been very helpful to us in terms of giving us materials
2 to use to help train our baristas on that. We do have a
3 relatively high turnover in terms of staff, so getting
4 people on top of that can be sometimes problematic, and
5 we do our best with that, but definitely there is a
6 barista education there that can take a little bit of
7 time.

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

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

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

1 people really do need to pay attention.

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

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

11 MS. MAYER: Thank you both.

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

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

23 MS. MAYER: It was just a happy accident that
24 it turned out that you're the official coffee of the
25 University of Washington.

1 MR. JOHNSON: And we're happy to be so.

2 MS. MAYER: And right across from my office.

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

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

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

1 kind of information was on the card and what was
2 revealed.

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

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

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

1 after the fact.

2 But let me give you a little video to
3 demonstrate what we actually did.

4 (The video was played.)

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

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

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

22 A lot of people ask me about, how do they
23 disable the contactless interface on the card? Mr. Ho
24 suggested the microwave. That's fine if you like to see
25 sparks, I suppose. I get a number of phone calls,

1 though, asking me, how do I do this? They've called up
2 their credit card issuing bank and they've asked not to
3 have the contactless, an enabled one. And an
4 interesting story came back.

5 One woman said she called up her bank, and
6 they said, we'd be glad to issue you a noncontactless
7 card. Came in the mail. She opened it up.

8 Investigated a little bit further. It was actually
9 still contactless. But she wasn't able to actually
10 tell, because how could you distinguish these things,
11 they're so pervasive.

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

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

24 And it's mainly going to center around three
25 issues, and that is of personal privacy, informed

1 consent, and consumer choice.

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

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

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

21 So we don't know what kind of information was
22 provided to him, but apparently one of the most educated
23 people with a Ph.D. was not able to comprehend whether a
24 card was contactless or not. So that's just one data
25 point for you.

1 One other interesting thing is about the card
2 holder name. I'm really glad that the card holder name
3 is being removed, at least from the consumer
4 perspective, because the consumer then doesn't have to
5 worry as much about their name being exposed wirelessly.
6 I would be interested in hearing more about what that
7 does for the other stakeholders besides the issuing
8 banks and the payment associations.

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

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

1 me give you another example of that.

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

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

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

20 It was implying, at least in my opinion, that
21 strong encryption was being used to protect this kind of
22 consumer information. But what it actually, I believe,
23 is doing is protecting it in certain locations but not
24 in all locations. In particular, it was not protecting
25 the contactless interface.

1 Okay. The third topic I wanted to touch on
2 was on the notion of consumer choice. So today I kind
3 of make this analogy of, the choice of consumers is sort
4 of like the airlines before the cost of oil got so
5 expensive, and that was, today you have a choice of
6 chicken. So today, the consumers have a choice, and
7 it's hard for them to make that kind of choice, so how
8 do they know what kind of card they're getting, for
9 instance.

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

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

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

25 So let me give you a couple more examples.

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

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

17 One example of that, I have an undergraduate
18 from Malawi this year, and he's doing a project this
19 summer on contactless, and I told him to play with it.
20 And he said, oh, I'm really excited about it, so I went
21 down to CVS and I wanted to use my AmEx, and the cashier
22 swiped it. And he said, no, no, no, no, I want to use
23 the contactless. And she said, okay, I'll swipe it
24 again. Then he said, no, no, no, no, void that
25 transaction; I want to use the contactless. So she

1 said, oh, okay, I'll void your transaction. And she
2 tried to swipe it, and so she started inserting it into
3 these holes, and she clearly did not know how to use the
4 card.

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

11 So in summary --

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

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

24 So analysts have proven that proprietary
25 systems from payment associations in the past have

1 failed to protect basic kind of information to the same
2 degree that you'll hear about in a moment on PCI.

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

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

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

23 Or are they going to just have some kind of
24 overarching incentive to make sure they get it right in
25 the first place before this really takes off. Because

1 today, the technology is rather -- it's not as widely
2 deployed as it will be, and when it is widely deployed,
3 it's going to be way harder to fix these problems. When
4 you move from 20 million to 300 million Americans, it's
5 going to be much harder to fix security problems and
6 privacy problems.

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

11 Thanks.

12 MS. MAYER: Thank you, Kevin.

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

23 MR. HO: You know, I don't think anything has
24 changed since then. I think basically the 128-bit
25 encryption is built in to, as was pointed out earlier in

1 a presentation, the UDK keys; they're loaded onto the
2 card, and that is where the encryption is. And at the
3 end of the day, when you're looking at speed and you're
4 looking at being able to turn something quickly, you
5 look for areas where you can -- you don't want to cover
6 up the whole thing; you want to be able to get it done
7 quickly, and so that's where it is.

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

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

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

1 MR. MCANDREW: All right, thanks.

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

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

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

21 I want to talk about what the ecosystem is
22 between merchant banks, member banks, acquiring banks,
23 card members, card holders, the PCI Security Council, so
24 talk about that at a high level once we understand what
25 is compliance and how is it being enforced and what is

1 it not covering.

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

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

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

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

22 About four or five years ago or so, each of
23 the card brands, Visa, American Express, MasterCard,
24 they all have their own operating regs, so you can go to
25 visa.com, you can pull up their Visa operating

1 regulations, or MasterCard, and they are still required
2 to enforce those. The problem is, those regulations
3 were enforced to the banks, and the banks enforced that
4 to the merchants, and the merchants were saying, hey, I
5 can't support three different ways. Visa does things
6 differently than American Express than at MasterCard.

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

16 Below them are the card brands. So all the
17 card brands have their own programs, but they also all
18 require all their member banks to enforce the
19 requirements in PCI. So they have something called data
20 security standard. They have something called the
21 payment application data security standard, which deals
22 with software and shopping carts which accept
23 information. And they also have the PED program, which
24 is the PIN encryption device program. So these new
25 programs are accepted and enforced with Visa,

1 MasterCard, American Express, JCB.

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

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

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

23 So what the banks have done is, now they
24 enforce those requirements on the merchants. So there's
25 about 1200 level one merchants out there, and these are

1 the largest merchants in the U.S., so they're merchants
2 that do more than 12 million transactions. And so the
3 payment card industry doesn't care about the value of
4 the transactions, because what they're interested in is
5 protecting card holder data.

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

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

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

25 Hannaford's is a large grocery chain in the

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

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

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

24 The important thing is, there's only three
25 programs that are being certified now, so when you say

1 that people are claiming to be PCI compliant or they're
2 claiming something, right now, and I've worked with a
3 lot of these different merchants, point-of-sale systems
4 are not really deemed as PCI compliant right now.

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

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

25 So if Tully's would have to increase their

1 coffee by three cents in order to pay for the cost of
2 their compliance programs and assessment, is that what
3 you as a consumer want in the end?

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

17 So let's talk about the threats that we have
18 now. So the threats with contactless, and we've gone
19 through a couple different ones here, if you look at the
20 statistics, in 2002, there's about 4,960 published
21 incidents of identity theft or accounts that were
22 compromised, and this was largely because there wasn't
23 disclosure laws in place. In 2005, that was 6.4 million
24 accounts. And last year, the estimates were about 162
25 million accounts. So chances are, half of us have had

1 something stolen. I've had mine stolen three times in
2 the last couple years. Once with the VA, with some of
3 that.

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

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

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

1 and then what can you do with it.

2 Right now, the type of information profile,
3 you know, names are not really considered areas, things
4 that you can sell. But things like PAN, which is a
5 16-digit number, Social Security numbers, driver's
6 licenses, those kind of go in the black market for
7 between ten and two hundred dollars or so an account,
8 depending on what you get.

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

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

21 The problem that we're stuck with right now
22 is that we have backwards compatibility. So when we
23 look at our credit cards right now, you have the
24 technology from 1950s, which is the embossed number; you
25 have the magstripe, which then was the next evolution;

1 you've got the CVV number, which is the next evolution;
2 and now you've got the contactless. So we've got four
3 different levels of technology that we're carrying
4 around and we haven't been able to retire those other
5 ones. As long as we have those other ones, it's going
6 to cause an issue.

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

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

22 When we look at kind of the U.S. in general,
23 there's about, I think estimates are about 400,000
24 payment readers, which is ten times more than anywhere
25 else in the world. So obviously we're big consumers,

1 and I can't remember exactly where I was looking at it
2 right now, but I think the average consumer has about
3 seven or eight credit cards, and then I think the next
4 country, I think is Brazil, which has one for every two
5 folks. So it definitely is interesting to kind of see,
6 as we get these cards and we're going to use them, what
7 we're going to do as consumers.

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

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

21 It's important to know because there's about
22 43 states now that passed identity theft laws, and those
23 laws define what sensitive information is or define what
24 personal information is very differently. So California
25 and Washington define them differently; Alaska is

1 passing one here shortly. So it's important to know
2 that, because when we talk about identity theft and what
3 we don't want disclosed, we have to know what that is,
4 because what you may see on a transaction, if it's a
5 masked number or if it's just your, you know, a Wells
6 Fargo account, it may not be considered sensitive
7 information; you may not be protected under state laws.

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

18 The problem again is the backwards
19 compatibility, and is it really designed correctly? And
20 part of an assessor, we go and look, for an example, we
21 see that credit card data is encrypted and we go and
22 look and we see that it's encrypted, and we ask where
23 the encryption key is, and the encryption key is stored
24 in the same database that the keys are, so that's
25 something of what the people that are designing the

1 systems and how they're going to enforce it are going to
2 do.

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

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

10 MS. MAYER: And I have one question.

11 MR. MCANDREW: Sure.

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

21 MR. MCANDREW: I'm not an attorney, so
22 there's probably a lot of attorneys can give that out
23 there. But I can tell you, what's interesting is, as
24 consumers, we were fed up with having our credit cards
25 stolen, and there's no federal kind of requirement, so

1 we've pushed those up, and the states have required each
2 one, and each one is different with the limitations on
3 it.

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

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

15 MR. MCANDREW: It's something to keep in
16 mind. Because from a security perspective, and you've
17 seen folks that can go out there, the limitation of the
18 two inches is because of the type of hardware they're
19 using in the connections, and the big concern out there
20 is that, I'm a U.S. citizen, I'm walking in a foreign
21 country, now people can go and detect me out there. So
22 there's a lot of folks that have gone through these
23 studies and said, look, we have that, I don't have the
24 option right now of not putting that RFID chip in my
25 passport, and I'm worried about kind of my security.

1 So there's definitely spectrums of what's
2 operationally easier and then also what's operationally
3 secure, and we've always got to try to find that happy
4 medium in between.

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

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

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

24 Overview. And today, there are 87 million
25 e-Money cards integrating mobile phones in circulation.

1 There are several major e-Money brands and card issuers.

2 Bordered in blue, you can see the number of
3 users. And Edy, which is highlighted, is our biggest
4 brand. But in terms of payment amount, bordered in red,
5 Nanaco is number one. So therefore, there is no
6 dominant player yet. And also, our company conducted a
7 survey in four major cities. Close to half of the
8 people surveyed said that they hold e-Money cards. But
9 they did only major cities where an e-Money terminal is
10 located in many stores.

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

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

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

24 The most important factor of the wider-spread
25 e-Money is the core business function bundle, because

1 e-Money is mainly used for small payment amounts, as
2 indicated on the left side of the table, and the income
3 to issuer is limited.

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

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

22 We estimated that the total amount of
23 electronic payment in 2007 was about \$85 million, and
24 75 percent of it was by e-Money payment. Based on the
25 current growth potential, we estimated that the total

1 amount of electronic payment will be over \$300 million
2 in 2012, and that of e-Money will be over \$200 million.

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

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

19 In contrast to this, the physical system
20 detects
21 not only IC chip but includes encryption OS application
22 standards. And it means that the (inaudible) optimizes
23 (inaudible) security. So this is a reason why many
24 businesses can launch their own services easily and
25 their services are secure enough.

1 Transaction data is encrypted with one-time
2 Password. It is similar to Visa and MasterCard. And
3 the key is the different in each application, of course.

4

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

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

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

21 The last reason shows general law. It
22 protects personal data based on OECD's principles. And
23 this provides more than enough protection for personal
24 data. We have not had e-Money payment data that was
25 stolen or used illegally in Japan. Personal information

1 such as name and telephone number is not necessary for
2 analyzing and for basic marketing.

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

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

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

24 The FSA is continuing to investigate the
25 registration for the various payment services, and

1 debate over the scope of coverage continues. There are
2 three main positions on this issue.

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

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

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

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

22 And this is the final slide. In this last
23 slide, I briefly look at the legal protection against
24 the business bankruptcies. This law, called the prepaid
25 card law, in short, treats e-Money recorded on a medium,

1 includes the card and mobile phones as prepaid cards.
2 Because a number of businesses can issue prepaid cards,
3 including e-Money in Japan, this legal framework is
4 needed to protect consumers from the risk of
5 bankruptcies of the issuer.

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

18 Thank you very much for your time.

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

24 MR. UEDA: Yes. Here is my transit card, and
25 on the back this card, there is a blank for signature,

1 but I didn't -- and also a railway company does not know
2 of who am I, only they know the ID, but they can
3 understand when I use it and from where to where, and
4 they can analyze what kind of doing I do, but they do
5 not know who am I. And they don't want to understand
6 who am I, so they don't request me to register my name.

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

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

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

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

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

24 Peter can speak to this, too, but there's no
25 reason issuers want to hide this. I mean, it's not as

1 though people can use it without knowing they're using
2 it, right? So every incentive the industry has is to
3 make sure that people know they've got this feature on
4 the card so they can go out and use it.

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

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

25 On the incentives, the assertion was made the

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

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

19 PCI and encryption, that's a very interesting
20 issue. PCI seems to be an issue with the merchant
21 community at this point, because, you know, while
22 financial institutions have been under an obligation to
23 keep information safe and secure for a long time, it's
24 just sort of getting to the merchant community and a lot
25 of them are not completely convinced it's really their

1 responsibility. But I think we're moving ahead in that
2 area.

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

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

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

20 DR. FU: I think the question is, is it the
21 same as having it embossed on the card. And the big
22 difference, there's a good analogy, and that is, with a
23 contactless card, it's as if you've tattooed onto your
24 forehead your credit card number and expiration date,
25 and the question is, can it be read?

1 Maybe if you're, you know, on the other side
2 of campus it cannot be read, but what if you're across
3 the room, can it be read? Well, we don't know. What if
4 the person has some kind of device that can extend the
5 read range? Well, we don't know.

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

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

21 And the answer is, you can go to a situation
22 where a card doesn't need to be present and you can try
23 to commit fraud, and we have issues with resolving fraud
24 in that kind of context; we're working on it. It's not
25 the kind of thing where you're going to fix the "card

1 not present" fraud problem by doing something in the
2 contactless space. It's a much bigger problem. When
3 you solve the "card not present" fraud problem, we'll be
4 able to address the contactless problem in a different
5 way.

6 One last thing --

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

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

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

13 MR. MACCARTHY: That will be fine.

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

24 Now, merchants don't like to take full
25 responsibility at this point for doing good security.

1 They've got issues with PCI, and some of those costs
2 might ultimately have to be passed on to consumers as
3 they do more and more security to protect information at
4 their own premises --

5 MS. MAYER: Okay, Mark --

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

9 DR. FU: Of course not.

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

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

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

23 Now, financial institutions have had to
24 safeguard data under Gramm-Leach-Bliley Act for many
25 years, and one of the things that I've actually said in

1 other panels that I've spoken on with FTC
2 representatives is that we would love to see a uniform
3 industry standard that applies to everybody in, you
4 know, not just banks, but everyone in the industry that
5 says you have to safeguard customer data. Is that
6 something that you would be supportive of it?

7 MR. MCANDREW: Sure, I --

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

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

23 So I definitely commend the institutions and
24 the card brands for pushing this out there, but the
25 problem is that the end merchants, like you say, if you

1 don't believe that the merchant pays for it, try working
2 with a bunch of different merchants, because they're
3 hiring folks like us to try to deal with this.

4 MS. GOLINSKY: (Inaudible.)

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

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

24 AUDIENCE MEMBER: I'll make my comments quick
25 here. I think it's clever that there's foil on new

1 cards as they're traveling through the mail; that's the
2 first time I've seen that.

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

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

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

22 I think as these new security features get
23 deployed, that will become easier, but most cards have
24 the exact same information on them. American Express
25 uses different credit card numbers encoded on the RFID

1 than on the magstripe, allowing them to do much more
2 advanced and sophisticated detection.

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

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

13 Thank you.

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

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

24 AUDIENCE MEMBER: So the current readers
25 emulate the magstripe technology?

1 MR. HO: That is correct. So the readers,
2 basically, it's magstripe data that's being transmitted.
3 However, there is a specific transaction code that every
4 acquirer must carry as a part of the mandates from the
5 association so that we can identify them.

6 AUDIENCE MEMBER: (Inaudible.)

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

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

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

1 doable?

2 MR. HO: It is doable.

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

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

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

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

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

23 MR. MCANDREW: From my experience, no,
24 because from an incident response perspective, there is
25 no response to that. Resources are being spent in

1 those. It's easier just to reissue a card and take
2 losses for a while.

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

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

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

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

22 But the reason why, first of all, contrary to
23 popular belief, we're not transmitting data off the
24 card. There is no power source on it. So it takes some
25 time for you -- because the power is coming from the

1 reader, and so it took me that long to get a read,
2 because you had to power up the card.

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

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

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

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

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

21 MS. REDFORD: Tom, I just want to echo that.
22 Earlier, it was stated and we want to make that very
23 clear, that the contactless application has simply the
24 same information as the magstripe. No, that's
25 absolutely not true. There's information laid down on

1 the magstripe, and there is an encrypted value
2 associated with that that we've been using for a very
3 long time at Visa, very successfully, to counteract
4 counterfeit.

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

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

23 MS. MAYER: I think we have time for at least
24 one more question, and I think we'll all be going to
25 lunch.

1 MS. GRANT: I want to preface my question by
2 saying that the consumer ends up paying, regardless. If
3 there is fraud, and also for preventing fraud, and it
4 doesn't really matter whether the merchant ends up being
5 liable or the issuer, the consumer ultimately is the one
6 who pays.

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

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

21 DR. FU: Can I adapt that? I'm curious, what
22 kinds of security options did Visa provide Wells Fargo?
23 What options were you allowed to choose from in
24 implementing on your device, and how does the consumer
25 know what choice you made?

1 MR. HO: At the time, we were given options.
2 Back then it was known as best practice whether or not
3 to name-mask, whether to shield the card. However, the
4 dynamic CVV was a requirement for to us implement.
5 There was no other way we can go to be certified. We
6 were highly -- it was highly recommended that we shield
7 both the name and in the mail stream, and we had
8 extensive risk management conversation, and it made very
9 good sense for us to do it, so we did.

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

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

1 technology.

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

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

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

17 And I think we've laid out some challenges
18 that, I don't know if they'll be answered, but they'll
19 certainly be addressed in certainly our last panel of
20 the day, so I hope everyone is staying around, and the
21 panel preceding that will be very interesting, as well.

22 Lunch, I guess which will also be very
23 interesting, if you would like to join us just for an
24 informal group lunch on campus at the dining hall at
25 Eight and McMahon, and Charles over here will be -- if

1 you want to follow Charles with just the group on the
2 tour to get there, it's about a ten-minute walk.

3 Thank you.

4 (Recess taken.)

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

MOBILE PAYMENT DEVICES

1
2 MS. RATTE: Okay. I think we're going to
3 get started now, everybody. Thanks for returning from
4 lunch. I know it was tempting to stay outside for a
5 little while.

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

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

19 MR. HANSEN: Thank you, Katie.

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

24 The mobile makes contactless payments more
25 than a swipe replacement. It makes the payment

1 experience intelligent, engaging, relevant, and trusted.
2 It offers security features and technical capabilities
3 that can improve the user experience, can authenticate
4 users and payment transactions, and can mitigate fraud.
5 And although there are many benefits that wireless and
6 mobile bring to contactless payments, a few of which
7 I've put on this chart, I'd like to just highlight
8 three.

9 First, the ability to know the customer and
10 where that customer is located. Second, reliable and
11 secure networks. And third, robust user interfaces.

12 Authentication is a term of art that we're
13 very familiar with in the payments industry. What it
14 really means is that you can determine that an
15 individual is authorized to make a certain transaction.
16 Authentication is required by most of the payments laws,
17 certainly by the payment association rules, and it
18 assists with fraud mitigation, consumer protection,
19 customer care, and other aspects.

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

1 in payments.

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

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

16 Just a note here, it's been very clear
17 through the morning session that we understand that RFID
18 technology uses a communication protocol that does not
19 rely on the wireless carrier's network. That's
20 independent. So in addition to the security features
21 that we've already heard today that just exist with
22 RFID, you can layer on top of that certain of the
23 security features baked into wireless networks to the
24 extent the payment system really needs to touch that
25 wireless network. And it may not, in too many ways, and

1 certainly not for the point-of-sale transaction where
2 it's really being read from a reader and the handset, or
3 from one handset to another handset.

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

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

22 My opinion is that the mobile improves on the
23 traditional concerns, in part because of the mobile
24 facilitates better disclosures and transaction
25 information, user and transaction authentication, access

1 controls and security features, and fraud mitigation,
2 among other things.

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

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

24 Despite those open questions, I think it's
25 clear that somebody will always be minding the store.

1 There will always be, just like in any traditional
2 payment system, one or more program providers who are
3 promoting and providing the payment service, the mobile
4 payment service, to consumers. And those program
5 providers will be responsible for consumer protection
6 and compliance considerations.

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

15 Thank you.

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

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

1 tracked?

2 MR. HANSEN: Certainly. If you haven't seen
3 it yet, you might look at the CTIA's Web site for the
4 location based services best practices guidelines. The
5 wireless industry, as a whole, put a lot of time into
6 anticipating these questions that might arise in the
7 consumer protection context and laid out a very
8 thoughtful set of guidelines and best practices that do
9 revolve around the two main principles of consumer
10 notice and consumer consent.

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 MS. RATTE: Okay. Now, we're going to hear
21 from Susan Grant, who's Director of Consumer Protection
22 for the Consumer Federation of America.

23 MS. GRANT: Thank you. I should start by
24 saying that contactless payment in general and mobile
25 contactless payment offers many potential benefits to

1 consumers. So we're excited by it. Clearly, mobile is
2 the Holy Grail of contactless payment. All the
3 forecasters say that this is what's going to drive
4 widespread adoption of contactless payment by both
5 consumers and merchants.

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

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

24 And consumers' privacy is not really
25 adequately protected by the legal regimes that we have

1 right now. We've got specific rules for telephone
2 companies in terms of what they can do with customer
3 information and how they can share it, and under what
4 circumstances consumers can opt out or what
5 circumstances require consumers to opt in for their
6 information to be shared with others. But of course,
7 the information doesn't need to be shared with others.
8 It could be used by mobile carriers in revenue-sharing
9 agreements with consumers to market them without ever
10 having given consumers' location or other information to
11 business partners.

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

22 So the one thing that is clear in this
23 confusing situation is that the phone or the PDA is no
24 longer a communications device. It's a device that has
25 a wealth of information on it and that can be used for a

1 variety of purposes, and consumers may not be aware that
2 sensitive information that may be in it can be used and
3 obtained in different ways.

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

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

23 It's great that the mobile providers can
24 provide things like PIN numbers and so on to give
25 consumers the protection that they need, but then my

1 question is, will that be the standard practice or a
2 required practice, or will it just be another best
3 practice that companies will adopt or not.

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

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

21 Children are a special concern, because while
22 children are not carrying credit cards and debit cards
23 around, they are carrying mobile devices around, and if
24 those devices are enabled to make contactless payments,
25 there need to be easy-to-use controls that should be on

1 by default and that shouldn't cost parents anything to
2 limit or restrict what their children can do. There are
3 concerns about over-consumption, not only by children
4 but by adults, and I think Jean touched on those this
5 morning, as well as things that people might do with
6 their devices that are things that by society we might
7 not want to have happen, like gambling using your mobile
8 device.

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

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

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

1 payment system that you want to use.

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

6 Thank you.

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

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

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

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

1 contactless payment.

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

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

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

21 It also would enable consumers to interact
22 with, say, smart posters. If I wanted to find out more
23 information about a particular item or a map, if that
24 poster is what we call a smart poster, I would be able
25 to touch that poster, maybe download some content or

1 interact with that poster to get more information. And
2 of course, payment is another opportunity that consumers
3 could potentially use this technology for.

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

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

17 (The video was played.)

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

1 we're not running as fast as you may think.

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

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

17 I don't know how much has been addressed
18 about the technology itself, but the contactless credit
19 cards utilize a secure element, and inside the phone
20 there is a secure element. It may reside in the phone,
21 on the SIM card, or on a memory card. And this is a
22 very secure protected area of memory that only the
23 application for the payment and certain keys are held.
24 And the credentials for the credit card are in the
25 secure element.

1 So when you make that transaction, the key is
2 never transmitted which produces the next CVC code. So
3 even if you did have a rogue reader to pick up your
4 credit card number and the CVC at that point, you could
5 never do the next transaction. The CVC would not line
6 up with the next CVC.

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

19 This could be taken further as technology
20 evolves, where biometrics such as fingerprints could be
21 used. So there's a lot of potential safeguards there.

22 As I said, the CVC code is highly secured
23 inside the secure element, and it is a dynamic code,
24 unlike a magstripe where it's -- I just had lunch; I
25 gave my credit card out to the waitress; she had my

1 whole name, card number, CVC, my signature, everything
2 was given away.

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

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

1 more than likely, you'll notice your phone missing
2 before you notice a credit card missing from your
3 wallet.

4 So that's my presentation. Thank you.

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

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

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

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

24 MS. RATTE: And what about Europe?

25 MR. WAKIM: There's opportunities in Europe

1 around, especially there's a lot more transit, where
2 people use metros every day or buses where there's
3 contactless tickets, so that's really the front line,
4 where U.S., more than likely, payment seems to be the
5 driver here. No more credit cards or debit cards.

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

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

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

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

1 solve all those problems.

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

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

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

22 So what happens in the way the contactless
23 payment in the mobile world is architected changes the
24 flow as follows, and this is to what Susan was talking
25 about. And it's architected for a good reason, by the

1 way. This is not something that just fell out for no
2 reason.

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

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

24 Therefore, financial institutions have to
25 work with operators to enable mobile contactless

1 payments. There's nothing inherently wrong with that.
2 It's theoretically very possible. Practically, it's got
3 a lot of issues. I'll highlight one of them, and there
4 are several.

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

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

22 But obviously, we know that this was not the
23 model that prevailed. This is the early '90s. In fact,
24 when I was trying to understand more about online
25 banking, I actually discovered something that was even

1 older, another example that didn't work. I don't know
2 how many of you have heard of Viewtron; I hadn't until
3 the day before yesterday. This was actually a service
4 provided in early '80s. It was in about 15 cities. It
5 was actually started by AT&T, with a couple of newspaper
6 companies, to provide content and services to customers.
7 They spent about \$15 million in 1980. If you're
8 interested in Google or Microsoft, that's probably worth
9 about five, six billion today. But nevertheless, it's a
10 model that didn't work, for obvious reasons. Again,
11 consumers don't have choice, what Susan pointed out.

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

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

25 Secure element can be a memory card. I don't

1 know if you've seen one of these. This goes inside your
2 camera sometimes, or a lot of the phones have these
3 these days. So this can be the secure element that your
4 card-issuing bank or association issues to the consumer
5 independent of this. Right?

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

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

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

22 This is data from April of this year. In the
23 United States, 57 percent of the mobile phones have
24 memory card slots, across all carriers. Globally,
25 that's a monstrous 600 million phones. And memory card

1 slots generally were associated with smartphones. Four
2 years ago when we started, there were two models
3 available with memory card slots. Now, it's
4 exponentially grown. It's available in a wide variety
5 of devices. And NFC phones -- this does not compare the
6 two. NFC has definitely a whole bunch of other
7 applications that have customer convenience beyond
8 payments.

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

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

22 What's important is in the long-term,
23 retaining freedom of choice for mobile contactless
24 payments is extremely critical, and the financial
25 institutions and carriers and payment associations have

1 to pay attention to this. I'm not sure how much
2 attention has been paid in the NFC forum. Up until, I
3 would say, middle of last year, memory card as a secure
4 element was still a discussion item. It was not really
5 committed. It has been at this point, so it is a viable
6 option. A technology has to be available, a viable
7 technology has to be available to provide this
8 independence, if you go back in history.

9 I'll stop with that.

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

18 DR. NARENDA: That's a very good question,
19 actually. And that's really where the SIM cards have a
20 significant advantage, because a street vendor in the
21 corner of China knows what a SIM card is.

22 The only way that the alternate secure
23 elements will be educated to the consumers has to be
24 through financial institutions and stakeholders who have
25 potential value in it in spending a lot of marketing

1 dollars to educate the customers. It can't be a
2 technology play. It really needs to be a use-case play,
3 explaining to consumers what options they have and how
4 they use it. There is no way around that; there is no
5 shortcut.

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

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

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

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

23 MR. VILMOS: Thank you. I was invited to
24 talk about the European experience, and I will do that,
25 but before I start, I would like to give some

1 perspective generally about mobile payment and this
2 mobile contactless technology, because it's much more, I
3 guess, than what you are talking so far about.

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

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

20 And I'm talking also about using the mobile
21 as an acceptance device. I know that it doesn't fit
22 with the present security requirements. I'm not talking
23 about open loop payment systems, but for closed loop,
24 small propriety systems, mobile can work as an
25 acceptance instrument.

1 But if you are talking about mobile payment,
2 you shouldn't just consider proximity transactions; you
3 should also consider remote ones. Because mobile is by
4 principle. It's a device which has remote communication
5 channels. So why not then combine it with value-added
6 functions like mobile banking, new services like sending
7 invoices, making time deposits, making realtime payments
8 using mobiles. So everything has to be considered
9 combined when we are talking about mobile financial
10 services. And obviously, it gives great new potentials,
11 but adds to the complexity and to the challenges.

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

20 But then it can be loyalty. It can be
21 excess. It can be event ticketing. It can be a number
22 of other services. And depending on the market
23 specifics, in one country it is going to be one service
24 which will lead the penetration; in another country it's
25 going to be a different one.

1 Now, if we are talking about a static
2 portfolio like this one, this is not very convenient.
3 So we have to give the choice to the customer to make
4 selections, delete existing services and download or
5 deploy or load new services. So it's going to be a
6 whole dynamic environment in the mobile handset, and
7 this is what is the real value proposition.

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

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

20 Europe is considered to be the most advanced
21 or the more advanced geographic region where mobile
22 communication is, with mobile communication concerns.
23 We have high level of mobile services, and mobile
24 financial services are really getting mainstream. We
25 have mobile banking, different basic or even interactive

1 solutions. I was just talking to someone during lunch
2 that we can transfer money from our mobile device to
3 merchants or to other people. We obviously make parking
4 payments from our mobile device. So mobile payment is
5 done, not the proximity one, but the remote mobile
6 transactions.

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

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

22 Now, the bad news is that mobile contactless
23 services or the introduction of mobile contactless
24 services is not going to be driven by the contactless
25 industry. It will follow a contactless acceptance

1 environment. When plastic cards, either transport,
2 ticketing, payment is already on the market, is
3 prevailing, then that's the time when mobile contactless
4 services will really mature and being introduced
5 commercially.

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

17 On the other hand, although commercially the
18 service is not available in Europe, it's going to come.
19 We have multiple trials. We have new trials. You hear
20 it in London with Oyster; that's the subway transport
21 card. Barclays, they have very successful trials there.
22 This is the largest one or one of the largest one in
23 Europe. France is very active. In several cities in
24 France, there are major trials, and those are very
25 unique. I guess those are the most complex ones all

1 over the world, including Japan, because this is the one
2 where the most players, the most active stakeholders are
3 involved and are incorporating mobile services. This
4 includes multiple mobile operators, multiple banks,
5 retailers, different handset manufacturers, so this is
6 really complex. This is really almost like a commercial
7 operation.

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

17 In all these trials, we see very good telco
18 and mobile network operator and bank operations. The
19 problem is that they are pretty much island solutions.
20 There is no interoperation between these initiatives,
21 propriety technology, specific handsets, so there's no
22 way from these specific solutions we will get a
23 European wide, overall, homogenous system. And the
24 solutions always need special technical environments,
25 because, as I said, it is not ready yet.

1 The question is whether people who are
2 involved in these trials like it and what effect the
3 trials have on the population. I have to tell you that,
4 generally, people don't care about these technologies.
5 We here in this room may be very interested in it; we
6 may like it; we know the benefit. But the general
7 population, first of all, doesn't even know what we are
8 talking about. Second, doesn't care.

9 Yesterday, I came through border control, and
10 the lady was asking me what am I doing here. I said, I
11 came for business. What kind of business? I said, I
12 came for a conference. What kind of conference? Mobile
13 payment conference. What? Mobile -- what type of
14 mobile payment? You know, you touch your mobile and you
15 pay. What?

16 (Laughter.)

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

1 contactless transport, the reception is a lot higher.

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

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

23 Now, more interesting, and it's a message for
24 the mobile operators, first movers may have a commercial
25 and marketing advantage, because over half of the

1 participants, they said they are even willing to change
2 their network operator if one is offering a service and
3 another is not. And they said that -- this was a trial
4 which was considered really successful, because people
5 were not doing one transaction and another one a couple
6 of weeks later, but they constantly purposely made their
7 payment transactions using their mobile handset. So
8 this is a good sign, but education, as was the previous
9 question, is kind of important.

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

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

24 Now, before I start talking about the actual
25 regulatory environment, we have to see that mobile

1 contactless payment purely from a transactional
2 perspective is nothing different from a contactless
3 payment using a card. An actual contactless reader
4 shouldn't even recognize the difference, whether I place
5 the card or a mobile handset to it. So from a
6 transactional perspective, risks are exactly the same.

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

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

24 And many other questions we still don't know.
25 As I said, we have trials here in the States, in Europe,

1 in the Far East, but in their complexity they are much
2 simpler than what we will see in the future when,
3 really, mobile contactless services will proliferate.
4 So we just need to prepare for it, have to consider it.

5 And just to raise a couple of issues which
6 we will actually face, we have privacy solutions,
7 data protection, but liability is going to be a key
8 issue.

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

20 So we have an ownership structure and
21 different parties involved in the issuance of the
22 application and the operation, so we will have a very
23 complex environment. There are corporations, liability
24 issues, that will have to be managed somehow. The same
25 thing which adds to the complexity that mobile financial

1 services really makes sense if you can view it on the
2 remote communication potential. Now, I wouldn't like to
3 get a payment card, like today, that you get it in the
4 mail; it's not going to work. So probably all of these
5 instruments, all of these service are going to be shot
6 over the air.

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

14 One other thing and I will finish it.

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

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

1 like that.

2 Thank you very much.

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

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

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

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

22 MS. RATTE: Okay. Now, I'd like to throw it
23 open to the audience. And anyone who has a question,
24 I'd like to ask you to identify yourself before you ask
25 it. So do we have any questions from the audience?

1 MR. MOORMAN: Dave Moorman, Director of
2 Retail Technology for PCMS.

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

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

1 be proactive and, actually, more importantly, reactive
2 to security issues.

3 MR. WAKIM: I can add from a mobile platform
4 perspective. Unfortunately, we're going down a little
5 bit the same path as the PC. There are mobile antivirus
6 software available, and it's one of the most popular
7 applications that is purchased on smartphones.
8 Companies like F-Secure, for instance, make mobile
9 antivirus.

10 MS. RATTE: Any other questions?

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

21 MR. HANSEN: I'll take that one. I think it
22 depends, and it depends on the particular
23 implementation. But in the end, the consumer will be a
24 customer of one or more service providers, and it will
25 either be a customer of the wireless carrier, be a

1 customer of a bank, be a customer of a transmitter, may
2 be a customer of an aggregator, taking a portal model;
3 you might log into a portal like you do on the Internet
4 today and access other services.

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

20 MS. GRANT: Just a quick comment. I think
21 that it's very important in that all the stakeholders
22 have a role to play, but my hope is that there actually
23 wouldn't be that many messages that we have to get out
24 to consumers, that a lot of the things that will protect
25 them in this space will be built-in and automatic so

1 that they don't even have to think about it, they don't
2 have to understand it. They're never going to be
3 techies. And it's all the same issues that we deal with
4 right now with PCs. It's just got to be made really
5 simple and built-in and automatic for consumers to use
6 it.

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

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

23 DR. NARENDRA: I have a short comment. In
24 terms of the responsibility of consumer education, it
25 will really rest on whoever is making transaction fees.

1 So in that sense, it depends.

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

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

9 MR. JOHANSON: Eric Johanson, the Schmoo
10 Group.

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

25 MS. RATTE: Thank you. Anyone else, any

1 final comments?

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

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

17 (Applause.)

18 MS. RATTE: And we'll see you back here at
19 3:30.

20 (Recess taken.)

21

22

23

24

25

1 **MEETING THE CHALLENGES: STRATEGIES AND APPROACHES**

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

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

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

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

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

1 might be:

2 What are the legitimate expectations of the
3 customer who makes use of a contactless payment system?

4 What should they expect in terms of the capturing of
5 the data during the initial transaction, the
6 transmission of that data from the point of purchase,
7 and what are the responsibilities of those who possess
8 and store the data? What can the customer legitimately
9 expect in terms of accuracy, security, access?

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

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

21 I took the liberty of Googling the names and
22 the organizations of our very distinguished panelists,
23 and I will try and give a little interesting
24 informational tidbit to start with, and then we will be
25 hearing from our panelists from my right on down.

1 First, we have Alissa Cooper, who is the
2 Chief Computer Scientist for the Center for Democracy
3 and Technology. According to their Web site, CDT works
4 to promote democratic values and constitutional
5 liberties in the digital era. With expertise in law,
6 technology, and policy, CDT seeks practical solutions to
7 enhance free expression and privacy in global
8 communications technologies.

9 Ms. Cooper.

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

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

24 I'm going to start with a little story, and
25 it sort of builds off of Dr. Fu's story from earlier

1 about the engineer who didn't know that he had a
2 contactless payment card.

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

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

1 point.

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

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

1 information has been a little bit vulnerable.

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

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

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

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

1 digital systems over the past decades.

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

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

25 We've been through some of these lessons many

1 times, and we should think about that moving forward.
2 This may be a new technology, it's different, you know,
3 you tap the card instead of swiping it, there's many
4 differences about it, but some of the underlying
5 security protections should be the same.

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

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

1 transmitted be random and dynamic.

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

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

21 Now, on privacy, I feel like we've heard a
22 lot about choice, and I completely agree with those who
23 spoke earlier who said that you should be able to refuse
24 the card; you should be able to -- if you get a
25 contactless card and you don't want it, you should not

1 be forced into using it. And it's good to hear that
2 some banks are offering that option, but I feel like
3 that's another thing where it's just like, seems like
4 should be universal.

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

10 And then as far as mobile is concerned,
11 thinking about privacy, the gentleman with CTIA was
12 talking about consent, I think even when you have
13 choices and you decide, yes, this is something I want
14 or, no, it isn't, it shouldn't be consent once and it's
15 forever. So if you buy your mobile device and you have
16 to decide, yes, I want to use contactless payment and
17 therefore every time I make a payment that information
18 is also going to go to the network operator or it's also
19 going to go to some application on the phone, that's not
20 true choice, because you're either saying, I can always
21 -- you know, every time I pay for something, this
22 information is going to get shared, or I just can't use
23 my phone to pay. So I think when we're thinking about
24 consent and choice, we need to think about true choices
25 and not this kind of false choices where it's all or

1 nothing.

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

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

25 I think on consumer education -- my fourth

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

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

24 Finally, I would just say, as always, the
25 good actors end up on these FTC panels, and I think, you

1 know, we heard this morning Wells Fargo had a choice,
2 should I take a more secure option, should I take a less
3 secure option; and they took a more secure option. But
4 the people who aren't up here are the banks that don't
5 offer choice or the merchants who are not making use of
6 the security features, and as we think about what to do
7 going forward, we need to think about the less than good
8 actors and not just the folks who are willing to come to
9 forums like this and talk all about all of the great
10 things that they're doing for consumers, because we all
11 know that it's a wild world out there and there's lots
12 of other players in this space who are not necessarily
13 meeting up to the practices of the folks that we've
14 heard about today.

15 Thanks.

16 MR. COVINGTON: Thank you.

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

25 Dr. Moorman.

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

4 MR. COVINGTON: And I teach hi-tech.

5 MR. MOORMAN: Well, thanks to the FTC for
6 having me here, and thank you for the promotion to
7 doctor.

8 MR. COVINGTON: I do it all the time.

9 MR. MOORMAN: We did get the title right. I
10 am the director of Retail Technology for PCMS, a global
11 point of sale, primarily software, vendor. And I'm also
12 wearing another hat, actually several hats today. One
13 is as the director of technology for that company. That
14 company, we're the point of the sword. We're the piece
15 of software that sits on that device and takes that
16 information from the consumer and then passes it along
17 the stream. So that's very much the emerging standards,
18 and where this is going is very much of interest to us.

19 I'm also a member of the Association for
20 Retail Technology Standards, ARTS, their governing
21 technical committee. And ARTS is a division of the
22 National Retail Federation. So I'm involved in the
23 development of standards. And ARTS is mainly about
24 efficiency standards, how to make data flow from one
25 retail application to another, not so much compliance.

1 But one of the things that PCMS and ARTS work
2 together on is a very successful standard called Unified
3 Pause, U-Pause, which is the programming standard for
4 retail devices. So when you swipe one of those legacy
5 magnetic stripe readers, that data, that track data is
6 passing through a standard interface that was designed
7 by those two entities. So we have a lot of stake in
8 this game.

9 I'm also here as a consumer, and I'm also
10 going to tell my consumer story about credit cards.

11 In fact, it was a coincidence, the day I was
12 asked to be a panelist I got a call from one of the
13 credit card companies -- which one was it? Which one of
14 you guys? It was MasterCard, and they said my card was
15 making the rounds buying televisions in Bangalore,
16 India, and were these valid transactions. And I said
17 no, and they voided the transactions; they actually
18 hadn't gone through.

19 But for that day, I was an un-person. They
20 said they'd overnight me a new card. And I was out
21 traveling, and all of a sudden I found out I had to go
22 back and put a different credit card, fortunately I had
23 one, on the hotel room bill and a number of other
24 things. I had to get online and do a whole bunch of
25 stuff so my life wouldn't come apart.

1 Coincidentally, a few months earlier, I had
2 been to a grocery store, to a self-checkout, and I took
3 out my wallet and I laid it down while I scanned my
4 items, and the disabling device that disables the theft
5 protection, like for DVDs, wiped out every magnetic
6 stripe in my wallet. And again, I became an un-person.
7 All of a sudden, I was not able to transact business; I
8 wasn't able to prove who I was. This is an example of
9 what I call Type 2 incident theft.

10 I think we've talked a lot about Type 1
11 identity theft, which is someone else stealing my
12 identity, but another type of harm is this Type 2,
13 where I can't be me because of the actions of another
14 party.

15 My point here is that real people are getting
16 hurt.

17 And one of the other stories I always tell my
18 nontechnical friends in trying to explain what I do in
19 the job is, I always point out the old science fiction
20 movies or the old James Bond movies where they overload
21 the computer and smoke comes out and it bursts into
22 flame and glass flies all over the room. And I always
23 tell them, I almost wish that happened; I almost wish
24 when computer systems didn't work, they would just
25 explode. Then it wouldn't have taken us ten years to

1 get a version of Windows that doesn't lock up.

2 Again, all due respect to the building.

3 My point of all of that is, real people are
4 getting hurt, in real ways, and consumers, and I think
5 that makes it appropriately the FTC's business to get
6 involved. And I predicted to the management of my
7 company a year ago, watch the FTC, because it's going to
8 happen.

9 Although I'm not going to talk extensively
10 about contactless payments as much as other people have,
11 I'm going to talk about more approaches and some of the
12 things I'd like to see the FTC doing. But we've already
13 talked about the fact that it's already here. If you've
14 got a cell phone in your pocket, some computer out there
15 in the world knows just where you are, and that
16 information can be queried.

17 So it's not a matter of if, or if ideas can
18 happen, it's when and, in fact, it's already happened.
19 We can either figure out how to regulate this smart, or
20 else it will end up getting regulated stupid. Let's not
21 wait until two senators get their name in the paper
22 about the privacy issue and pass some act that is going
23 to make an emergency measure of getting a handle on this
24 topic. One of the big keys here that we've got to work
25 towards is balancing innovation against standards, and

1 one of my themes is, where does the standards community
2 play in this whole thing, and what is FTC's role in
3 that.

4 Another story: I got pulled over by a police
5 officer once, and he said, you know, you're driving on
6 the wrong side of the road. And I said, no, I'm not
7 not; I'm an innovator.

8 So my point is, somehow we have to have this
9 balance against what is society -- what standards do we
10 need to make society work and make all of this work for
11 the consumers and without derailing innovation. And my
12 concern is, at some point if this becomes a senior
13 political issue, that we're not going to have the time
14 then to make that proper balance between innovation and
15 keeping the economy going.

16 Some of the drivers and things I've heard
17 this morning that as a technologist kind of jumped out
18 at me and I said, well, I don't know if I buy that. One
19 is, phones are programmable. To use the mobile payments
20 as an example, these are devices, they've got a little
21 operating system in there, and it's a matter of time, in
22 fact it's already happening, that viruses are going to
23 get in there. And as somebody pointed out, once money
24 becomes a motivating factor and not just annoyance, the
25 viruses will explode.

1 I'd like to point out that there is a large
2 body of hackers out there. I do a lot of training and a
3 lot of consulting, and a lot of the people I'm training,
4 for example, for the implementation of my product, are
5 offshore developers. We are training a small army of
6 offshore programmers in how these systems work. And
7 Alissa used the term "security by obscurity." There is
8 less and less tolerance, and there must be less and less
9 tolerance against the idea of, oh, well, nobody will get
10 in there and figure out that microcode or how to do that
11 buffer overrun. That's been proven time and time again
12 that that's just not obscurity -- security through
13 obscurity is just not security.

14 I heard some things about proximity: Oh,
15 well, you have to get it two inches from the reader.
16 That goes right up there with another of Mr. Gates'
17 comments: Nobody will need more than 64K of RAM ever.

18 The only thing that is true in life is three
19 things: death, taxes, and the miniaturization of IT.
20 And something that can only be read from two inches away
21 today will be readable from two miles away tomorrow. So
22 we do need to be forward thinking about what is the
23 technology turnover rate.

24 And one of the things there is, and I'll talk
25 more about this in a minute, to represent the merchants'

1 viewpoint, merchants have very ponderous
2 infrastructures. It's very expensive for them to turn
3 over their technologies in store. So I hear people say
4 things like, oh, all you've got to do is apply this
5 patch, or all you've got to do is put another 128
6 megaRAM in there. Well, it's not the cost of the 128
7 megaRAM; it's the cost of sending somebody out to the
8 store and opening up the box and putting all that extra
9 memory in there and dealing with all the issues with
10 drivers and whatever. So any mistakes that get made in
11 the implementation of these infrastructures, retailers
12 have to live with and have to amortize those costs over
13 a very long period of time.

14 I want to talk a minute about an article and
15 some of the things that came out of it. I encourage you
16 to go Google this. There is an article out there by
17 Information Week called "PCI and the Circle of Blame."
18 "PCI and the Circle of Blame." It was published in
19 February of 2008, and it gives a really good overview of
20 the liability and political issues swirling around PCI
21 and the liability.

22 Coincidentally, a month later we had the
23 Hannaford breach that you've heard about some. What was
24 significant about the Hannaford breach, a grocery store
25 on the East Coast? Several things. One is, they were

1 PCI compliant. They had the stamp of approval. Yet
2 they got breached anyway.

3 The other thing about it is that it wasn't
4 one breach of 4.5 million credit cards. It was 4.5
5 million breaches of one credit card at a time. And I've
6 heard several things up here about, well, we're not
7 worried about the one-offs, the one-card breach, because
8 that doesn't scale. Well, yeah, it does scale, because
9 what somebody did is they penetrated the system, they
10 inserted a Trojan that listened between the
11 point-of-sale software and the acquirer software and
12 picked up that credit card as it traveled through the
13 memory of the computer. Very innovative attack.
14 Somehow, somebody used a virus to propagate it, so it
15 was actually -- it wasn't somebody hacking into the big
16 data center in the sky and getting all 4.5 million
17 credit cards downloaded; it was a little thing that was
18 listening to every single transaction and sending out
19 those credit cards over a period of time.

20 So look at that article, and it talks very
21 much about the circle of liability that's forming. I
22 happened, by the way -- in a previous life I was
23 originally an accountant and an auditor, a financial
24 auditor, so I know the world of auditing and the
25 requirements that auditors have as far as

1 professionalism and doing their job for their clients.
2 And I guess there's no nice way to say it; PCI and the
3 auditing, because of the Hannaford breach, is kind of in
4 a mess right now, because everybody is trying to figure
5 out, what does it mean? Is Hannaford off the block
6 because they were compliant? Well, what is the
7 liability for the QSA? So everybody is trying to figure
8 out what this circle of liability is going to be.

9 It's nice that there is a feedback loop, but
10 right now it's very inefficient and it's very
11 unpredictable. So retailers are kind of flipping a coin
12 as to what to do and how to invest in fixing this
13 problem.

14 I'll also make note that PCI is a great
15 start. I should note that pcisecuritystandards.org,
16 although it's an org, it came out of the PCI world, out
17 of the payment card industry, and so it's done a lot of
18 fine work, but it doesn't, in my opinion, accurately
19 reflect all the stakeholders: the consumers and the
20 merchants and the credit card industry.

21 So I talk about the merchants and some of
22 their quandaries and some of the things they've got to
23 worry about. Well, I already said they have ponderous
24 infrastructures, so whatever gets put out there in
25 thousands of stores, they have to live with and they

1 have to eat the cost if there's patches or upgrades that
2 need to go out.

3 Something that was mentioned earlier was
4 signature capture versus not signature capture for items
5 over \$25. We have the problem of employee -- our own
6 employees can be our biggest security vulnerability with
7 employees pocketing cards, skimming, those kinds of
8 things.

9 Do we go contactless or not? We have to deal
10 with offline issues. The network isn't ubiquitous to
11 the point where you're always online. Retailers have to
12 make a decision: When the network is down, do they take
13 the credit card and hope it's not a fraud? What do they
14 do there? I deal with those issues every day.

15 What I'm trying to get at here is, merchants
16 are in a really tight bind right now, because they have
17 to compromise between service level and security. And
18 each retailer has to kind of guess where they want to be
19 on that spectrum.

20 To use an example, compare this to an
21 airline. We would never say to the airlines, it's
22 entirely up to you whether you do maintenance or not or
23 whether you put gas in that airplane or not. We don't
24 let people in the airline industry play with people's
25 lives, and what we need is -- and I'll get to my point

1 in a moment about standards -- we need to make the
2 retailers, help the merchants get off the hook by giving
3 them clear standards that everybody is going to play by.

4 I'll go on and come back to that.

5 I'd like to look at other regulatory models
6 that have worked. I use my plane analogy. We have a
7 National Transportation Safety Board that looks at
8 problems. Whenever an airline goes down or there's ever
9 a problem, the NTSB, as a third party, investigates and
10 says, what went wrong? Their job is to say, where did
11 the breach occur based on certain standards that are
12 previously set? And over time, for all of its
13 disadvantages, our airline industry is actually pretty
14 good. I mean, most of the time, I looked it up, there
15 are about 50,000 flights a day in the United States, and
16 they almost never crash.

17 In the appliance industry, we have
18 Underwriters Laboratory, which certifies our appliances
19 so they don't burn our house down. So there are many
20 regulatory frameworks out there that I think we can
21 learn from. And one of the things that I think is
22 lacking in IT in general, and particularly in this area,
23 is the ability of arbitrating what is a foreseeable
24 versus a not foreseeable problem.

25 If you're familiar with Palsgraf versus Long

1 Island Railroad, in 1928 it established foreseeability
2 as the standard for liability and negligence. We don't
3 have anything yet where we can definitively say, when
4 something goes wrong, how are we going to go in there
5 and figure out who really is responsible for that
6 breach.

7 Microsoft has a really good term for this.
8 They call it surface area. What is the surface area of
9 the system. They take it from stealth. You've got an
10 airplane, and then when they came out with stealth
11 technology, they said surface area is now much smaller
12 than the actual airplane. Now it's the size of a
13 sparrow. And what we need to do is come up with a
14 regulatory framework that will over time reduce the
15 surface area for these army of hackers to get into.

16 To recap, there are people who are really
17 getting hurt; that makes it the FTC's business. We have
18 to balance innovation against keeping the economy going.
19 And we have some established regulatory models.

20 And I'd like to make a call to action. I'd
21 like to see the FTC get involved in bringing all of the
22 parties to the table and all of the stakeholders to the
23 table to compel some standards that have some muscle and
24 some teeth to it. We saw many cases up here of "he
25 said, she said," of, well, you can't get a PAN off this

1 thing. Well, beep, there it is, and can that be used
2 for creating bogus credit cards.

3 Whenever you deal with security, you have to
4 talk about what are all the different -- security isn't
5 one thing, you have it or you don't. You have to talk
6 about what are the different access threats, and that
7 can become a very emotional argument. I think FTC has
8 to come in and be involved both proactively in the role
9 of standards and reactively in the role of forensics, to
10 start to bring some accountability to the situation.

11 It's a journey we're on. It's a journey we
12 all need to take together. But we've got to move that
13 surface area smaller and smaller incrementally in real
14 ways.

15 And my time is up.

16 MR. COVINGTON: Thank you, David, and my
17 apologies for the errata.

18 Kathryn Ratte is Senior Attorney for the
19 Division of Privacy and Identity Protection with the
20 Federal Trade Commission.

21 Kathryn.

22 MS. RATTE: Thank you. And my apologies to
23 everyone in the room who has to listen to me on two
24 consecutive panels. I'll try to keep my remarks brief.

25 I'm here to now to give you a very brief

1 overview of the Federal Trade Commission and how we
2 address issues raised by emerging technologies through
3 our existing enforcement authority.

4 If there's one message I want to leave you
5 with, it's that the FTC has the tools to address this
6 type of emerging technology and others using our
7 Section 5 authority, which is broad and flexible, and we
8 are out there on the beat, and when we see practices
9 that deceive consumers or harm consumers, that's when we
10 step in. So now would be a good time to give the
11 standard FTC disclaimer.

12 The views I'm expressing are my own and not
13 necessarily those of the Federal Trade Commission or any
14 individual commissioner.

15 So, as I mentioned, we're an enforcement
16 agency, and our responsibility includes enforcement of
17 laws related to data security and consumer privacy, and
18 these are very high priorities of the Federal Trade
19 Commission. Although my focus today is on law
20 enforcement, that's just one piece of what we do. I
21 wanted to mention that we do take a multidisciplinary
22 approach to protecting consumers. In addition to
23 rigorous law enforcement, we conduct outreach directly
24 to consumers to give them the tools to protect
25 themselves against emerging threats, and we also provide

1 guidance for industry to help them understand their
2 obligations under the law.

3 So getting back to the law enforcement,
4 although we enforce some sector-specific laws in the
5 area of privacy and security, including
6 Gramm-Leach-Bliley, our primary enforcement authority
7 comes from Section 5 of the Federal Trade Commission
8 Act, which broadly prohibits unfair or deceptive trade
9 practices. And the Section 5 authority is very broad.
10 We reach a wide range of industries, with some notable
11 exceptions, including the banking industry, and I
12 believe John is going to give us a little bit of an
13 overview of what the regulatory landscape is for banks,
14 but that is one area that we do not regulate. We get
15 just about every everybody else under the sun.

16 In the privacy and data security context, the
17 FTC uses its Section 5 authority to make sure that
18 businesses keep the promises that they make to consumers
19 about their privacy and data security practices. That's
20 kind of the deception piece of our statute. And also to
21 address business practices that cause or are likely to
22 cause harm to consumers, including the failure to have
23 reasonable security measures in place to protect the
24 privacy of sensitive consumer data. So you can't
25 deceive consumers and you can't harm consumers. That's

1 Section 5 in its very, very most basic summary.

2 Because our deception and unfairness
3 authority is so broad and flexible, we frequently find
4 ourselves at the forefront of new technologies, like the
5 one we've been discussing today, also others, and our
6 standard in this space is reasonableness. We require
7 companies to have reasonable security, to have
8 reasonable privacy practices.

9 So, accordingly, this means that we can
10 address emerging threats without technology-specific
11 regulation. We're looking at the overall reasonableness
12 of a business' practices, not whether they have one
13 specific security measure in place or, you know, one
14 magic bullet. We realize there isn't one, and we
15 wouldn't be in the best position to go out and
16 anticipate that, anyway. We're looking at the totality
17 of what they're doing for privacy and data security.

18 I'll give you a couple of examples.

19 In 2005, we brought a case against BJ's
20 Wholesale Club, which is an East Coast discount
21 warehouse. For those of you West-Coasters here who
22 haven't heard of BJ's, it's like a Sam's Club. And they
23 experienced a major security breach in which the credit
24 and debit account information for many of the customers
25 who had shopped at its stores was accessed by a hacker.

1 And in that case, we alleged that their
2 security practices as a whole were unreasonable and
3 resulted in harm to the consumers whose accounts were
4 compromised. We alleged that BJ's has failed to take
5 into account the specific security risks posed by, among
6 other things, the use of an unsecured wireless network
7 at its retail stores. Their failure to secure the
8 wireless access points is what allowed the hacker to go
9 into the system and get access to that card holder data.

10 We were able to allege that this failure was an unfair
11 business practice because it resulted in the harm to the
12 consumers.

13 We had a more recent case announced in March
14 of this year against TJX, the TJMaxx discount clothing
15 store. In that case, hackers were able to obtain the
16 credit and debit card information of approximately
17 450,000 TJX customers that were stored on the system.
18 And again there, the FTC alleged that TJX failed to
19 implement reasonable security measures to protect the
20 customer information it collected and stored, including
21 failing to implement readily available security measures
22 to limit access through the wireless access points at
23 its stores.

24 So in both cases, the wireless issue was one
25 of a laundry list of security failings. There were also

1 issues about storing card holder data beyond the time
2 that they should have been, and there were encryption
3 issues, as well. It was really a failure of the entire
4 system.

5 But I use those to illustrate the point that
6 we didn't need a specific regulation saying you need to
7 secure wireless access points. Because we look at the
8 totality of the system, we can address these risks to
9 consumers as they come up.

10 And I also wanted to echo a point that was
11 made earlier, that the point of collection of consumer
12 data, which is a lot of what we've been talking about
13 today, the contactless card, the first read, that's just
14 the first part of the whole data life cycle. When the
15 FTC looks at a company's practices, we don't just look
16 at how is information collected, but how is it stored,
17 are there access controls, is it disposed of securely.
18 You know, we look at data retention issues. That piece
19 of it is the start of a whole process, and we expect to
20 see reasonable security throughout the process.

21 I'll just close by saying that the FTC has
22 been monitoring the potential impact of technologies
23 such as RFID and contactless payment on consumers, and
24 we won't hesitate to use our existing Section 5
25 authority in appropriate cases if we become aware of

1 practices that deceive consumers or otherwise harm them.

2 And I'll leave it there, and look forward to
3 your questions. Thank you.

4 MR. COVINGTON: Thank you, Kathryn.

5 John Carlson is a Senior Vice President with
6 the BITS/Financial Services Roundtable.

7 John.

8 MR. CARLSON: Thank you very much. It's a
9 pleasure to be here. I also want to thank both the FTC
10 and Bill Gates' father, whom this building was named
11 after, because if it weren't for Bill Gates, BITS would
12 not have been established over 12 years ago, and it was
13 in response to a comment he made to a group of CEOs
14 where he referred to bankers as potential dinosaurs, and
15 I saw earlier in the day we had a funny Far Side graphic
16 of a dinosaur smoking. And I think that brings together
17 to me a number of different themes that are important
18 for this event.

19 One is the role of regulation and where it
20 has limitations and where it's very effective.

21 Second is, there's a very strong role for the
22 industry to solve the problems and to address the issues
23 at the forefront.

24 And then third, there is longer-term
25 strategic issues which you really need to keep in mind,

1 in building on what Dave Moorman had to say regarding
2 innovation, that you can't be so fearful about how the
3 technology could be used in nefarious ways that you
4 don't allow it to move forward and gain some of the
5 benefits that are out there.

6 And I think Dr. Littman pointed out the
7 important point of costs and efficiency and things of
8 that nature. And our industry, our society, is becoming
9 so squeezed in terms of trying to eke out additional
10 efficiencies and gains that are out there as we have the
11 capacity to do that, so it's important not to hamper
12 ourselves in terms of moving forward.

13 So let me first talk a little bit about --
14 first let me explain what BITS is, since many people
15 don't know. We are associated with the Financial
16 Services Roundtable. We focus on the technology issues
17 that affect our member companies, which are the hundred
18 largest financial services of banking, insurance, and
19 securities. We have over the years focused an enormous
20 amount of attention on security, on fraud reduction and
21 identity theft. We actually established about five
22 years ago an Identity Theft Assistance Center which
23 helps victims of identity thefts to restore their good
24 name.

25 We also focus on outsourcing and vendor

1 management related issues, which when we're talking
2 about this, we're really covering all three of those
3 areas: security, vendor management, and fraud. And we
4 have experts in our member companies that gather
5 together on a regular ongoing basis to talk about how do
6 we solve these problems. And invariably, we spend a lot
7 of time trying to figure out, well, how do we work with
8 our critical partners, since many of these problems
9 cannot be solved by an individual company; even if you
10 take a very large company like a Citigroup or a JPMorgan
11 Chase, there are issues that have to be resolved on an
12 industry wide basis.

13 And so we spend a lot of time -- in fact, we
14 spent a great deal of time out here in the Seattle area
15 working with Microsoft on software security related
16 issues several years ago. We've tried to work with the
17 Internet service providers on things having to do with
18 fishing or e-mail authentication and things of that
19 nature.

20 So there's a really important role, both in
21 terms of what the industry can do to come together to
22 try to solve some of these issues and problems, and
23 there's also an equally important role for government to
24 be thoughtful. So I must hand it to the FTC for holding
25 this forum, to bring people together to talk about it.

1 I also would encourage the FTC to work with
2 their peers within the broader government in terms of
3 the Federal Communications Commission, the financial
4 regulatory agencies, because each of those bodies have
5 important roles to play. Even though the FTC doesn't
6 have, as Katie mentioned, oversight over financial
7 institutions, it does have oversight of the service
8 providers that financial institutions rely so heavily,
9 both in the United States and increasingly around the
10 globe. So everyone has a role to play in terms of
11 trying to move this forward.

12 Let me talk about regulation. The financial
13 services industry is, without question, the most
14 regulated industry in the United States. It's regulated
15 both in terms of safety and soundness, and increasingly
16 on operational risk, which includes information security
17 and fraud and consumer compliance and things of that
18 nature.

19 The regulators have built upon what I believe
20 is a very solid foundation in the law the Congress
21 passed in 1999, the Gramm-Leach-Bliley Act, which the
22 financial regulators took a very bold step in terms of
23 developing a rule that was risk-based, that was
24 flexible, that was kind of a continuous improvement
25 theme in terms of how do you solve this problem, that

1 it's not going to be a one-shot deal, it's going to be
2 an ongoing basis. And at the time, the OCC was one of
3 the authors of that rule, so I'm very proud of it in
4 terms of I think it's had a prominent staying power.

5 The regulators have also done a lot in terms
6 of trying to come up with more flexible guidance,
7 supervisory guidance. They're not regulations, even
8 though the industry often times responds to them as if
9 they are. An example of that would be a few years ago,
10 authentication guidance, which said you must enhance the
11 authentication. Many people interpreted it as you must
12 have two-factor authentication, although that's not
13 exactly what the regulators said.

14 The regulators have also over the last 15
15 years been thinking about what sort of impact electronic
16 money and banking will have on law enforcement,
17 supervision, the actual manufacturing of money, things
18 of that nature. And so in preparation for this, I
19 actually went back to a conference that the Treasury
20 Department had sponsored with all the Treasury Bureaus,
21 which in and of itself was a unique experience in terms
22 of having all the Treasury Bureaus work together, and
23 they developed a conference and a paper in which they
24 laid out in the paper the following quote:

25 Government must be careful not to overreact

1 to or stifle new innovations that can greatly benefit
2 the consumer and the American economy. Government
3 should take advantage of marketplace solutions to issues
4 where appropriate. To do this, and at the same time to
5 be in a position to act appropriately, it is important
6 for government to maintain expertise in electronic money
7 and payments developments and to consider carefully
8 major questions presented by these developments.

9 And I think that still holds in terms of
10 thinking through this problem. We can't be fearful of
11 what the consequences might be, but we need to be
12 forward thinking in terms of how these technologies may
13 be used in unintended ways.

14 So my conclusion from listening to today's
15 panel is that the issue of contactless payments is
16 somewhat contained, given how it's being used and how
17 the people that are trying to develop this market are
18 intending to use it. They see it as a low-value
19 transaction to substitute for cash, a way to facilitate
20 and get people through lines, to add value for coffee
21 merchants or sporting events, et cetera. So in that
22 context, I don't see a lot of significant issues with
23 respect to how companies have developed systems and
24 developed controls and applied the appropriate security
25 controls.

1 Where we may run into some issues is expanded
2 beyond that, expanded beyond what was actually intended.
3 And that's where government needs to be thoughtful in
4 terms of, what are the signals that you want to send to
5 the payments providers, what are the signals you want to
6 send to the cell phone manufacturers and the device
7 manufacturers, as well as what needs to be done to work
8 together to solve these sorts of issues having to do
9 with liability, which is a huge issue. And again,
10 people in the financial services industry have a very
11 large chip on their shoulder with regard to liability,
12 because they typically bear it in terms of the losses
13 that come through.

14 Increasingly, the customers are starting to
15 bear it through identity theft, and that's where the
16 government has really stepped in and the Federal Trade
17 Commission, in particular, has played a major leadership
18 role in saying, look, we've got to develop solutions to
19 address the identity theft issue.

20 So I'm going to stop there, because there's
21 been a lot of things discussed today that I think are
22 very solid points, but that one issue that I was most
23 concerned about was the point about innovation and that
24 we need to be mindful that we get great benefits from
25 the innovation, but we also need to be forward thinking

1 in terms of how do we protect consumers as technologies
2 are used in ways that we're not anticipating even today.

3 MR. COVINGTON: Thank you, John.

4 Dr. Tadayoshi Kohno is an Assistant Professor
5 at the Department of Computer Science and Engineering
6 here at the University of Washington.

7 Dr. Kohno.

8 DR. KOHNO: Thank you very much. As Dr.
9 Covington said, yes, I'm an assistant professor here.
10 I've actually been in the computer security and privacy
11 industry for about ten years. For those of you who know
12 the industry a little bit, I used to work with Bruce
13 Schneider's company back when we only had basically four
14 full-time cryptographers and that was it, and that's when
15 I worked with them; also another company called Sigital
16 (ph.), and while I was there, I ended up doing some
17 consulting work with Visa and MasterCard and a whole
18 bunch of other companies.

19 So that's where I started my career in
20 computer security. Then I went to graduate school and
21 got my Ph.D. in the area of cryptography, so how do you
22 design protocols mathematically to provide certain
23 levels of privacy or integrity, et cetera. And I also
24 analyzed a whole large number of real systems both in
25 the academic world and when I was a consultant, such as

1 voting machines and other types of RFIDs.

2 I should start off by saying that actually I
3 really am not in the contactless payment space; I'm in
4 the computer security and privacy space. And my
5 research touches a little bit on contactless payment
6 systems, but I kind of want to start off by talking
7 about security and privacy in general.

8 And so the first question that I always try
9 to ask my students or other people when we're talking
10 about technology is, you know, raise your hand if you
11 know exactly what security and privacy means for
12 contactless payment systems.

13 So either everyone is being shy or people
14 realize that we actually don't know what security and
15 privacy means. I think that's one of the main issues
16 that I'm very glad to see this type of forum and other
17 types of forums address.

18 If we step back a little bit, one thing that
19 we see is that often times in the media they portray
20 security as this binary. You know, they say these cards
21 we have are horribly broken; they're very insecure. Or
22 they say that they're perfect. But in my view, security
23 and privacy is not a binary. There's no such thing as
24 perfect security. What we really need to be asking is,
25 who are the parties involved in this particular type of

1 technology, what are their goals and what assets do they
2 value, and does it provide an adequate level of privacy
3 and security under these circumstances.

4 And many other people today are talking about
5 this very complex ecosystem, and I think that's actually
6 a very important point to keep in mind. If we take this
7 approach that computer security and privacy is a binary,
8 we might end up in a world where we just kind of dive
9 into a bunker and say, you know, let's get rid of all
10 technology and stop innovating.

11 On the other hand, if we take the other end
12 of the spectrum and say there's no problems with this,
13 we might end up innovating and taking technologies in
14 new directions that actually end up putting us in a much
15 worse scenario.

16 And I believe neither is right. Really, we
17 need to step back and say again that security and
18 privacy is not a binary; but what is this landscape, who
19 are all the parties involved, what are their interests,
20 and can we figure out a way to balance all these
21 interests.

22 So I might say that there's really this
23 seesaw between security and privacy and cost and
24 usability and time to market, and we really want to
25 figure out the right balance to the seesaw. And now

1 here's an opportunity to say, well, what is the right
2 balance, what does this balance mean? And actually I
3 don't know the answer to that, and I think it's great to
4 see these type of forums where we get more and more
5 people together to talk about this and try to figure out
6 what is the right balance for contactless payment
7 systems.

8 So one thing that I think I would -- let's
9 see, trying to keep on track.

10 So I think towards getting to a point of
11 figuring out what is the right balance, I think it's
12 very important for everyone to be very open about how
13 their systems work or what their requirements or
14 criteria should be. And so for computer scientists, I
15 think this means that we need to not just look at the
16 technology but try to understand the business factors
17 affecting the contactless payment systems. But at the
18 same time, I think I would like to see the contactless
19 payment industry being more open about exactly what
20 protocols are they using, not necessarily relying on
21 proprietary systems, because as we know from the past,
22 proprietary systems have a tendency to have been broken,
23 but to be more open about their processes and exactly
24 how their systems work.

25 My second point that I wanted to make is that

1 there are many possible -- if we look at these
2 technologies, they're making possible ways of innovating
3 that we haven't thought of yet, and I would like to see
4 more interaction about what are the actual challenges
5 that people are facing and how can we innovate.

6 And so earlier today I saw lots of discussion
7 about how challenging it is to replace the back-end
8 systems. So we have this large deployment of these
9 point-of-sale readers, and the actual costs, I think
10 Dave Moorman talked about the actual costs to replace
11 these readers can be very expensive. And so the
12 question we have in our research group was, well, what
13 could we do to actually improve the security and privacy
14 of these contactless payment systems without actually
15 changing the back-end readers and without also changing
16 the usage model of these contactless payment cards.

17 And one approach we came up with was actually
18 kind of talked about by others before, but we actually
19 implemented it, was to take a passive RFID tag and put a
20 little bit of accelerometers or motion sensors on them,
21 and what we can now do is that we have can have this
22 passive RFID tag in our wallet and walk around, and if
23 anyone tries to read it, they will not actually be able
24 to read it. But as soon as we take it out and take our
25 wallet out and wave it or do a certain small pattern in

1 front of the reader, the contactless card itself will
2 get power from the reader and then will detect the
3 motion and say, am I doing the characteristic motion
4 that would allow me to communicate, and under these
5 circumstances and only these circumstances it would
6 actually transmit.

7 And so this is one potentially cheap way to
8 improve the privacy and security properties of these
9 contactless payment systems without actually changing
10 the back-end systems. So this is just one example of
11 one type of way of innovating. I suspect there might be
12 many other types of ways of doing that, but I want to
13 make sure we keep these in mind.

14 The other thing that Alissa talked about
15 earlier that really drives home to me was the point of
16 consumer education, and here's another opportunity where
17 technology might be able to help with this education. So
18 you could actually think about making some technology
19 that you would wear in your pocket or some other type
20 of, maybe wear on your wrist or wear on your belt that
21 would actually tell you when your RFIDs are being read.
22 Or it could actually, you know, this little thing that
23 you have on you and if you get a new RFID -- if you go
24 to a store and they give you RFID tags, they'll tell
25 you, by the way, do you know you have these RFID tags

1 near you.

2 Other things that we might consider doing as
3 a community is setting up public kiosks where, as a
4 community service, some organization might set up
5 kiosks, and then you walk by and they say, by the way,
6 do you know you have these RFID tags, and I just read
7 your names.

8 So like I said, my area is not actually in
9 the contactless payment space. My area is computer
10 security and privacy broadly. And I know I have five
11 minutes left; I actually won't use it all.

12 My main points is that I would like to see
13 more discussion about what does security and privacy
14 actually mean in this space, and how can we come to some
15 sort of middle ground that's in everyone's best
16 interest. And again, several ways of doing this: One
17 is, of course, computer scientists and computer security
18 experts need to compromise and they need to say, well,
19 we're not going to expect perfect security because
20 perfect security doesn't exist; we need to understand
21 what your threat models are so that we can come up with
22 technologies that fit those threat models.

23 At the same time, I would like to see
24 industry be more open. Again, I'm not in this industry
25 so I apologize if I'm insulting someone because you

1 already are open, but I'm hoping you will be more open
2 and not use proprietary algorithms but tell us exactly
3 how your systems work so we don't get into confusing
4 scenarios where it's "he said, she said" and we don't
5 actually come to a consensus.

6 And lastly, I really do think there's great
7 opportunity to innovate, and by coming to a better
8 consensus about the practical constraints that the
9 industry is facing, whether it's back to maybe we can't
10 read or play back systems, et cetera, computer
11 scientists can then say, okay, well, under these
12 constraints, this may be how we can innovate a solution.

13 And so that's it.

14 MR. COVINGTON: Thank you, Dr. Kohno.

15 Paula Bruening is Deputy Executive Director
16 of the Center for Information Policy Leadership of
17 Hunton & Williams, LLP.

18 Paula.

19 MS. BRUENING: Thank you very much, and thank
20 you to the FTC for inviting me to be here today and for
21 giving us such a gorgeous day in Seattle.

22 There's always a challenge in being the last
23 person on the last panel, because in some ways you feel
24 like everything that you had planned to say has already
25 been said, but I do think that in being asked to talk

1 about transparency and consumer education, this really
2 is not a bad place to sit, because it allows me to
3 highlight some of the things that have already been said
4 today and maybe expand upon others.

5 I think it's pretty clear, both from what
6 we've heard today and for all of us who have been
7 watching the evolution of this technology and its
8 deployment over the last few years, that there is
9 something about RFID technology that despite all the
10 benefits that it may well offer us, it makes people
11 uneasy.

12 It's an invisible technology. It's used in a
13 way that's somewhat passive to the consumer, in some
14 instances, where the consumer doesn't necessarily have
15 to engage in its use, although that is not the case in
16 contactless payment systems. But I think that it raises
17 the specter of surreptitious surveillance and tracking
18 in a way that other technologies, even though they may
19 actually be functioning in similar ways, they don't
20 raise that concern for consumers. And so I think this
21 is an area where transparency and notice about the
22 technology is really, really important.

23 And I think that in the case of RFID
24 technology, you're talking about transparency and notice
25 in two ways.

1 First, notification about the fact of the
2 technology itself is really important. You want to
3 build trust with your customer base, with consumers. If
4 you want deployment of this, you've got to be really,
5 really clear and honest and open about what is being
6 used.

7 And the second is notice and transparency
8 about any kinds of ways that this technology is being
9 used to facilitate data collection and data sharing and
10 use.

11 And when you talk about contactless payments
12 in closed systems, you really are talking about a
13 technology that's being used in a certain kind of way
14 with financial institutions, but I think today we've
15 heard about, you know, use of this kind of technology in
16 things like cell phones where you're looking at the
17 possibility of data sharing between different vendors to
18 allow different kinds of services to be offered, and so
19 you're talking about the privacy of data collection and
20 use, as well as the concern about RFID technology
21 itself.

22 I think there's been a lot of discussion
23 about notice over the last few years, about notice being
24 challenging, that perhaps consumers don't really
25 understand notices; they're difficult to write; it's

1 complicated; you can't make a consumer read the notice
2 that you send. And I think there's some truth in many
3 of those observations, but I think there still is a very
4 important role for transparency in notice, and they
5 remain fundamental to sound, responsible technology
6 deployment and data collection.

7 And they really encourage an enhanced
8 engagement by the consumer when you're talking about a
9 technology that is somewhat silent and not so obvious.
10 It also encourages disciplined data use and, obviously,
11 as Katie said, it opens the company up to scrutiny about
12 how the technology is being used, and it allows for
13 regulation in a flexible and nuanced kind of way.

14 But I think overall it's important to think
15 of it as a means to build trust with your consumer base,
16 and also it's fundamental to the guidance that's been
17 put out there about RFID deployment, much of that
18 guidance which has been developed by companies and
19 industry.

20 I think in the case of RFID, this can be
21 particularly challenging because of the nature of the
22 technology; and in many cases, RFID, when you look at
23 different kinds of deployments, is out there in the
24 environment; it's not necessarily something that you can
25 put your hands on immediately.

1 But as I said before, in the case of
2 contactless payments, I think this is the easy case.
3 This is a closed system. This is a situation where
4 there are many, many opportunities to engage with the
5 consumer, to give them information: at the time that
6 they apply for the card itself; when the card gets sent
7 to them, there's an opportunity there; with the monthly
8 statement. And the companies that deploy this are
9 sophisticated companies that have Web sites that can
10 inform consumers on an ongoing basis, because, as we
11 know, this is an evolving technology; we're finding
12 different applications and different ways that it can be
13 used.

14 One proposal that has been out there, and I
15 think that has been picked up by this industry, is to
16 have some kind of a logo that immediately indicates to
17 the consumer that there is this technology in place. I
18 know that there are projects under consideration in
19 Europe and within U.S. industry to put that kind of logo
20 out there. I think that such a logo is a good idea, but
21 I think that behind it there really needs to be
22 additional information that gives the consumer more
23 information about the benefits and the possible risks of
24 the use of this technology and allows them to make
25 better decisions about safeguarding their card and

1 making good decisions about where they leave it and
2 making sure that they take it with them when they get
3 out of the cab.

4 So when we talk about transparency, we're
5 talking about compliance with applicable laws in this
6 case, but also about establishment and compliance with
7 sound information practices. It's real a dual kind of
8 challenge when it comes to this kind of technology,
9 particularly when we are looking forward to a world
10 where data is going to be used among vendors that are
11 all coming together to make a service or an application
12 available to the consumer.

13 And I think in closing, I would just like to
14 say that, looking ahead, it's important to remember that
15 this is really, to my mind, the cutting edge of a world
16 that we're creating that is going to have a much more
17 ubiquitous deployment of RFID technology, not just for
18 contactless payment but for all kinds of uses that
19 engage the consumer both in active and in passive ways,
20 that we're creating environments where we're going to
21 have sensor-based and radio technology offering us all
22 kinds of benefits and also presenting us with lots of
23 different kinds of challenges, and it's going to be
24 really important that we take on this question of notice
25 and transparency and creating a consumer base that's

1 really active and engaged and understands what they're
2 involved with and what they're using as we go forward
3 and create this new world.

4 Thanks.

5 MR. COVINGTON: Thank you, Paula.

6 Questions? Bob? Bob, could you identify
7 yourself and --

8 MR. CALAFF: (Inaudible.) It really may be
9 too early to ask this question, but where do we go from
10 here? I think we have shared a lot of good information
11 and opinions, and do we focus on best practices next?
12 Do we focus more -- a little more deeply on where the
13 technology is headed? Other things? I mean, I throw
14 that out just for consideration. Thank you.

15 MS. RATTE: You have actually set up an
16 excellent bridge to Eileen Harrington, who is our Deputy
17 Director of the Bureau of Consumer Protection; she'll be
18 talking to us a little bit about next steps, any minute
19 now.

20 MR. MACCARTHY: Mark McCarthy with Visa.

21 One quick comment on this whole question of
22 standards and regulation. I think we're pretty
23 comfortable with where the FTC is right now on this
24 concept of reasonableness as a way to approach security
25 issues. You're using your UDOP authority. Maybe it

1 would be a little better if you had explicit guidelines
2 to do stuff on safeguard rules as opposed to UDOP. But
3 the general idea that there should be a reasonable
4 standard makes a lot of sense.

5 Once you start to get below that and say,
6 well, maybe we should all have uniform and very concrete
7 standards that all of the payment systems should live up
8 to, or the way they're doing in Europe right now,
9 they're trying to have uniform standards for all RFID
10 applications, as if there's something in common between
11 supply chain and payment systems and health care and all
12 the other RFID applications. That's probably a mistake;
13 or if you're going to do it, it's going to be at such a
14 high level of abstraction it won't be concrete
15 information. So that's a comment on security practices.

16 Alissa had a great point on mobile payments
17 and mobile banking, which is actually in play right now
18 at the Reserve Bank of India, which is, we all want to
19 have a situation where bank customers can get the
20 underlying banking services that they want and need
21 regardless of the mobile carrier, so you don't have to
22 sort of shop around for a mobile carrier at the same
23 time you're looking for banking services, but it's kind
24 of tricky to get there. I mean, you may be able to cut
25 a deal with one mobile carrier first, and the ideal may

1 be to have a deal with everybody, but you don't want to
2 have a requirement that says banks can't provide mobile
3 banking services to anybody unless they're prepared to
4 work with all carriers, because then one carrier who
5 doesn't want to sign a deal would stop the whole
6 process.

7 So it's not clear how you get to the goal,
8 but it's a goal that we think makes a whole lot of
9 sense, and if there's going to be some further
10 conversation and discussion about that, it's something
11 that I think we would like to participate in.

12 And the last comment is on Hannaford. I
13 actually checked with my corporate relations people.
14 That's a very delicate situation that we're in right
15 there. We can't comment and don't comment on the
16 compliance situation of anyone with PCI, but it's
17 important to emphasize there's a difference between
18 actually being in compliance and validating compliance.
19 Very, very delicate situation.

20 MR. COVINGTON: All right. I'm afraid at
21 this point, our time is up. I want to thank our
22 panelists.

23 (Applause.)

24 MS. HARRINGTON: Well, that and each of the
25 panels today have been -- that was and the others have

1 been just terrific.

2 I think this is a wonderful venue for a
3 really important session. We at the FTC really believe
4 in what our current Chairman Bill Kovacic talks about as
5 public consultations. We have been doing these kinds of
6 sessions for almost two decades. We hold gatherings
7 like this, whether we call them workshops or town halls
8 or hearings, to educate ourselves and consult with
9 others in that process in the most public way, to say
10 there are important issues here, we need to dig deep, we
11 need your help to learn what it is that we need to know
12 in order to do our job as well as we possibly can.

13 So this particular public consultation grows
14 out of the Tech-ade hearings that the commission held in
15 2006, "Protecting Consumers in the Next Tech-ade,"
16 looking at technology issues that were likely to raise
17 consumer protection implications and issues over the
18 next decade. And contactless payments specifically, and
19 RFID more broadly, is one area that we looked at
20 Tech-ade and we think we need to keep looking at and
21 keep drilling down on.

22 What happens next?

23 The next phase of the contactless payment
24 RFID public consultation will continue on September
25 23rd, 2008, when the FTC joins with the Department of

1 Commerce at a workshop on RFID technology that will be
2 held in conjunction with a European commission
3 Department of Commerce symposium that's going to be held
4 in Washington. The September 23rd event will be a
5 half-day event. It will be held back in Washington, as
6 I said, not here in Seattle. It will be at the FTC's
7 New Jersey Avenue Conference Center, and there will be
8 more information up on our Web site very soon about
9 this.

10 I can't tell you how pleased we are to be
11 able to get out of Washington. You know, the weather
12 there stinks; it's pretty good here. But more than
13 that, there is just a richness about doing these
14 consultations around the country and not always staying
15 in Washington. Now, I know we have a lot of people here
16 who schlepped all the way out from Washington or New
17 York, but we've got people here who are from this part
18 of the country, as well, and other parts of the country,
19 and we think that that's very important, and we think
20 that it's particularly important that we join with the
21 academy when we can to do these consultations, and to
22 that end, we are so grateful to the University of
23 Washington, School of Law, and to Bill Covington for so
24 generously joining with us and hosting us here today.

25 We also are so grateful to the staff who have

1 worked hard and will continue to work hard on this
2 issue, and our team on the RFID issue cuts across time
3 zones and includes Julie Mayer, Katie
4 Harrington-McBride, and Katie Ratte, who really have
5 been the key people on this issue at the FTC, one from
6 Los Angeles -- one from our Los Angeles office, one from
7 our Seattle office, and one from Washington, DC. So we
8 thank them for their incredible work on this issue, now
9 and always.

10 (Applause.)

11 MS. HARRINGTON: And also Chuck Harwood for
12 his leadership here in the northwest region, for taking
13 this issue on in the northwest regional office
14 portfolio. The lead on this issue in the agency is
15 right here in Seattle. We also want to thank others
16 from the Seattle office who have helped out today:
17 Charles Gust, Josh Kohls, Samantha Woo, Denise Pruitt,
18 and David Goldfarb. Thanks to -- where are all of them?
19 There are others. There they are. Thank you.

20 (Applause.)

21 MS. HARRINGTON: So thank you all for coming.
22 I think this has been a rich session. I think we will
23 continue inviting you to learn and discuss with us.
24 These are important issues, and we always want to make
25 sure that as we move forward, that we not act in a way

1 that is precipitous. We don't want to squelch
2 innovation, but we also are very serious about using all
3 of the tools that are available to us to protect
4 consumers when consumers need protection.

5 And so we look forward to continuing to
6 discuss these issues, and we'll see you in September in
7 Washington, I hope. Thanks very much.

8 (Applause.)

9 MR. COVINGTON: We have one more
10 announcement.

11 MS. MAYER: We have this facility courtesy of
12 Bill Covington and the clinic and the law school, but we
13 can't really host you, but we would love everyone who
14 has made the trip, certainly, to join as many of us as
15 possible for drinks at the Big Time Brewery; it's on the
16 Ave, University Avenue, just one block west of here on
17 41st Street. So if you want to make the walk, it's a
18 beautiful day, hope you can join us. Thanks.

19 And thank you all for coming, again, and
20 participating.

21 (The proceedings adjourned at 4:57 p.m.)

22

23

24

25