TRANSCRIPT

PROOF POSITIVE:
NEW DIRECTION FOR ID AUTHENTICATION

PANEL 7 &
CLOSING REMARKS OF LYDIA B. PARNES,
DIRECTOR, BUREAU OF CONSUMER PROTECTION,
FEDERAL TRADE COMMISSION

APRIL 24, 2007

>>NAOMI LEFKOVITZ

All right. Thank you. We are going to begin our final panel, next steps, where do we go from here? And the idea that we were thinking about in putting together this panel was that after having all these issues raised in the last day and a half, that we would then think about what are some practical solutions? What are some practical steps that we can move forward? So the idea here is not to have -- we're going to have the panelists give some of their presentations, but then we are really looking for a dynamic discussion. Not the formal sort of question-and-answer format we have had so far, but really have a dynamic discussion and get people to bring forward their thoughts and their ideas.

I want to make sure that Robin, you bring your question up again because this is the perfect panel for that. We didn't want to cut you off at all. And so I just want to take one step back. Because yesterday we started off pretty high level. We were talking about theories, about identification systems. And what we're talking about is a means to reduce identity theft in this workshop. And there are many ways to reduce identity theft, but in this case obviously through better identification and authentication.

But we don't want a system that creates an equal or a greater problem in other areas. Privacy, for example. That is why we started off the way we did yesterday to be cognizant of -- I think about Simon saying one of the problems is if you put forward the objective as only solving identity theft, that doesn't necessarily carry an identification system.

Perhaps I'll put forward this thought, that because perhaps it's when you build something focused solely on identity theft you might come out with a system that doesn't take into consideration these other areas, like privacy and things Paul Trevithick and others were saying about proportionality and how much information you have to give in order to conduct any particular transaction. So I just want to put those thoughts out there. That even though we have talked about these other areas of privacy, ultimately in this setting we're trying to think about ways to reduce identity theft, but not open the door to other problems.

So with that, I'm going to turn it over to Jim. I should say we have got Jim Lewis from the Center for Strategic International Studies. We have Greg Crabb from the United States Postal Inspection Service. We haven't heard much from law enforcement in this, so we thought this would be a great time to bring in that perspective. And then we have Jeffrey Friedberg from Microsoft, its chief privacy architect.

>>JAMES LEWIS

Thank you, Naomi, and thanks to the FTC for inviting me to speak. Let me say I'm glad to see the strategy. I think it's very helpful. The last question was right on. I think we need to talk about what is the role of government. Because as we were discussing during the break, you need both government and private sector and if you don't get the mix right, you're stuck. And one of those things they asked me in preparing for this was that I try and inflame you, so I'm going to try and do that a little bit and we'll see if it works. So, where do we go from here?

I think there are two central problems when I think about this. I'm very much focused on the Internet and on digital identification. How do you determine the trustworthiness of this assertion that you make over the Internet or over a network? And what is, basically as you heard in the last panel and what you've heard yesterday, an untrustworthy environment.

Another problem I think we need to pay attention to is, how do we adapt what are basically paper processes that we have developed over the last century to what are now digital and networked applications. We have made some progress. This strategy, for example, is a move in that direction.

You heard this before. I'm just going to do it quickly to go through the slide. The main point I would like to call your attention to is the role of government. If you don't have a good, strong, government process for confirming the identity that your family gives you, nothing else works.

And then you also have to ask, how do I transfer these government processes, whether it's a Social Security number or a birth certificate, whatever, how do I transfer them to some other kind of credential that I can then use in a commercial setting? Where are we in authentication? For me, I'm entering my 11th year working on authentication problems. I thought this was the picture to express my feeling. (Laughter.)

We have a lot of things going on in the authentication space. And there are some things we can draw from that. The first is, and this came up a little bit in the last panel, one size does not fit all. People will not want a really strong, robust credential for everything they do. In some cases, you want to have anonymity or pseudo-anonymity. Right now we might have too much of that, but we need to blend.

The second thing you have heard consistently is trust is expensive and people don't want to pay for it. In fact, in many cases it's easier to eat the cost of fraud than it is

to build in the trust. And this is again a theme we have heard before. We have what we call liability dodge ball. Which is, if I issue a credential and it's misused, who is liable? So one of the things I have seen happen in authentication for the last few years is everyone tries to dodge liability. I'm not liable for somebody else's error. That's reasonable, but it's a draw back. It's one of the things you need to think about. It's one of the things maybe only government can fix. Whether that's the courts or whether that's the Congress. The allocation of responsibilities within our ID management system here in the U.S. is unclear and you have a lot of contests.

And finally, you have what I call the coalition of the timid. And a way to think about this is automobiles. When automobiles were first introduced, I have used this one before so some of you may have heard it, they were scary. You had these dirt roads and people were used to horses and the horse was intelligent and if it saw you it probably wouldn't bump in to you. So cars were scary. What do you do with cars? So the answer was you have somebody walk in front of the car waving a red flag so people would know a car was coming and it wouldn't scare children. That's kind of how we understand these problems. We always start by asking ourselves -- there's a very vocal minority that says -- what are the problems I'm going to have to deal with?

I was at an event a couple of months ago where someone said that the Real ID Act – this was one of the speakers – the Real ID act was the first step towards an American Gestapo. Unfortunately those attitudes are very common.

I thought I would mention PKI. You have heard a lot about it. I'm a big believer in PKI and have been for many, many years. What are some of the issues? You need to think about the core credentials. These are the things that the government issues you. We don't have a very good process for doing that. It is getting somewhat better. What is it that lets me know how you are going to identify yourself? The key for me here is, how do you start networking these things?

A problem in the U.S. that I don't think Japan or Norway has is that we have a federal system and so you have dozens of entities that are issuing your identity-confirming documents. We're just beginning to network these things so something issued in one state can be checked against something issued in another state. So figuring ways to exploit network technologies out would help us in improving core credentials.

Interoperability: none of the systems I think work very well together that we have now, particularly on the digital side. A few years ago GSA had an interoperability laboratory and they looked at a bunch of different authentication technologies. What they found is none of them were interoperable. Things have gotten better since then, but finding a way to create interoperability is crucial for this, particularly in a large society like the U.S. and particularly as we begin to think about international applications.

How will we interoperate with something issued in Norway or the European Union or in Japan? Thinking about the rules for exchange of trust. There's a technical level to interoperability, but there's a trust level too. Just because I get a credential from

you doesn't tell me how much I can trust it. The most I might have is a brand name, and even that I'm not sure about. What are the processes that lay behind your issuing that credential? If I don't know those or if I don't have a way to assess them, if I don't have some kind of standard or guideline, I may not know how much I can trust your credential. If it's from a bank I can probably assume that it's relatively trustworthy. If it's from someone else, maybe I don't know.

Some of the things we need to think about are, what are the rules for authentication? This includes what Naomi has mentioned. We'll need rules for privacy. If people aren't comfortable that their privacy is being protected, they won't play. We need rules for how you opt in or opt out. I would prefer an opt-in system because that would help you deal with some of the objections. You're worried that Real ID is the first step towards the Gestapo, don't get one. That leaves me free to move ahead.

We need to think about how to assign liability. Not an issue that we've resolved. Finally, we need to think about enforcement, and I think some of the things we saw in the strategy are helpful on the enforcement side. The question that we heard from NTIA from the Department of Commerce was, what's the role of government? And for me, we need to think about who is it that has the lead on solving some of these issues? This is not a problem that either the private sector or the government can solve by themselves.

So one of the things we want to think about is who gets to assign responsibilities. Who has responsibility for what issue? Just leaving it sort of to the market hasn't worked. I myself wrote a paper in 1996. I said we didn't have to worry about authentication because the market would take care of it. So clearly I was wrong. Now we have to say, why has the market not provided this? And some people might say well, if we just wait another ten years, the market will get there. It's possible. But we could then frame the question as, how do we accelerate better identity management, better authentication, in the U.S. and elsewhere? Some of that is to assign responsibilities.

Government plays a key role. I would like to come back to that. On the interoperability side, what you've heard before is government should not get into the standards business. Government should not dictate technologies. You can see this in other countries. The Germans, for example, had a digital signature standard, not very widely adopted. Other places have looked at digital signatures. If you say there's one technological solution, and we all must use it, that's not going to work.

Finally, going back to this issue of rules, who is going to set the rules for the identity management system we have? It has to be a blend. The government can do certain things, the private sector can do certain things, and they need to find a way to work together.

What would be my next steps? If it was me, I think that's the title of this panel, fix some of the core credentials. Whether that means Real ID, whether that means HSPD-12, whether that means making everyone get a passport, think of a way to get

some sort of solid basis on which we can build identity. We do not have that yet. The thing that's used in the United States is primarily the driver's license.

I think the price has gone up. That's the good news. But a couple of miles from here there's an open air market. It used to be about 300 bucks, now I think it's gone up, it's like 700 bucks now, but I can get you any driver's license you want. You want to be George Bush, you want to be Osama Bin Laden, you pick. Just tell me the name, and I'll get you a Social Security card to go with it. So we need a better process for how the government issues those crucial credentials at the beginning.

We need to develop a way for the government and the private sector to cooperate. Perhaps the FTC could be the vehicle for that. There might be others. We need to have privacy safeguards. I know you heard a lot about that from Ari. You know if you don't have these privacy safeguards people won't use these things, at least in the U.S. That might be different in other countries. You need to have some sort of standard of trust. How do I know how much I can trust this credential? We have now a faith-based trust system. And while I myself am comfortable with it, it doesn't appear to be working. So some sort of standards. Who sets the standards? Some mix. Is it the banks? Is it the credit card companies? Is it the government? It's got to be a blend.

And then finally, think about where we need legislation. Whether that's assigning liability -- none of you worry about credit card fraud very much because your liability is covered, right? You're only liable up to 50 bucks and most credit card companies will eat that. Perhaps we need some sort of liability coverage for authentication. We need to think about whether the credentialing rules we have are enough.

Real ID, which I might be the only person left on the planet who likes, is a useful step in that direction. The fraud and privacy measures -- certainly the FTC strategy does a lot on the fraud side. You'll see other steps, I think, going along.

And finally, on privacy, the larger debate about whether we need some sort of improved privacy system in the U.S., some sort of single standard, authentication plays directly into that. If you can identify people securely, it's a good way to protect their privacy.

Let me conclude with a few statements. Commercial solutions -- I think this gets to the last question. Commercial solutions which, I think, are the basis by which we should build out better authentication will only work in an adequate government framework. You've heard the highway metaphor several times. You need the stop lights, you need the pavement, you need the curbs, you need the traffic lights and the rules for people to be able to operate commercially. So only if the government creates the framework will you see authentication work.

You'll need to accommodate diversity. There will be no one size fits all, at least not for the next ten years. Maybe at some point we'll reach a situation where we can lock in on a single technology. Interoperability will not happen naturally. Or it will not

happen naturally at a pace where we will live to see it. Interoperability includes the means to exchange trust. How do I know how much I can trust your credential? How do I know how trustworthy it is? How do I measure that trust? And those are things we have not yet worked out. There's progress in these areas, but we need more.

The components of trust, strong government documents and processes, adequate technologies for credentialing, and a framework for trust. A framework of rules that says who has liability. How do I determine what trust is? So I would see this as a place where, to end by answering the question, government is an enabler, and it's a guider, but it's not going to be the normal role of government as a monarch decreeing something, but government perhaps organizing and helping the private sector move in the right direction. Thanks. (Applause.)

>>NAOMI LEFKOVITZ

I have to cheat for a second here because I wanted to give a bit of context to Greg before he speaks. You would have heard from one of our panelists who was unfortunately ill yesterday about consumer behavior and opinions from surveys conducted by his institute. One thing he would have said is that, in asking what institutions consumers had the most trust in, in the public sector it turned out to be the Post Office. In the private sector, it was the banks. So I had to cheat a little bit here and set you up.

>>GREG CRABB

Thank you very much, Naomi, and thank you. I'm with the government and I'm here to help. (Laughter.) Thank you for allowing me to present my law enforcement and my limited views on countering identity crimes through the U.S. Postal Service.

These are my views, relative to when I present views relative to the U.S. Postal Service. They're my views and not necessarily the views of the agency. Briefly, I'm a program manager responsible for cyber crime investigations in the Postal Service's global investigation division.

I'm going to take a few minutes to explain what I have learned relative to the use of identity information to conduct schemes against consumers, merchants, and financial institutions. The basis of my experience has come through a shared investigative intelligence initiative with the FBI. Through this initiative I have worked with countless international law enforcement officers, government, private industry, and others to address crimes against consumers and businesses across the United States.

Through our shared investigative intelligence initiative at the National Cyber Forensic and Training Alliance, we monitor the activities of thousands of cyber criminals engaged in account takeover schemes, false application schemes, identity theft, credit card fraud investigations, brokerage schemes, spam, phishing, you name it, we're

engaged in it. And generally, we refer to this organized group as the International Carder's Alliance. However, their activities go well beyond credit card fraud.

Under the umbrella of Interpol and with law enforcement from over 30 countries, we collectively work under the operation name Operation Gold Phish, to target cyber criminals around the world engaged in network sales. The activities have included a number of arrests in Eastern Europe, West Africa, the European Union, and the Middle East.

How many of you have seen the movie Borat? Wow, actually some people will admit to that. (Laughter.) In so many ways that movie is so wrong, but in many ways it's an excellent portrayal of cultural prejudice. The film seems like a somber exploitation of prejudice, yet it has men running naked through hotel hallways, drunken frat boys, street kids willing to provide some coolness tips, and so many other things that are so wrong. But in the film Borat refers to a Trojan horse. But as the audience leaves the theater wondering whose prejudice has been exposed, the question of where the real Trojan horse is lingers, as a fake Kazakhstan anthem accompanies the credits across the screen.

And what he's done, he's crafted an intricate invasion of America in the form of a movie -- on the surface a laugh-out-loud comedy, and inside, an exposé of the audience itself. As I left the movie alongside my lead analyst at the National Cyber Forensic and Training Alliance and a close colleague in the FBI, we felt as if we had been hacked.

And that is exactly what the people that are pictured on this screen and in the title, the subtitle Borat, the Cultural Learnings of America For Make Benefit Glorious Anarchy of Cyber Crime.

These criminals are making a mockery of the cultural tendencies in the United States around identity. And the criminals sit behind computer systems in Eastern Europe and West Africa, across the European Union, and are making a mockery of our financial infrastructure for organized crime and terrorism financing. And unfortunately, I don't have a lot of time to talk about my passion, which is the investigation of these criminals, but I think we need to learn from these criminals on how to protect our infrastructure. Because we can make the best systems in the world, but from a consumer ease of use perspective, the same reasons why those systems are easy to use, these individuals are out there trying to exploit those vulnerabilities. Or see them as vulnerabilities to be exploited actually.

You don't want me to stand up here and sing the national anthem. But I am going to tell you what we need to learn about these crimes to understand how to better deal with them. The criminals expose an underbelly of vulnerability across various layers of remote commerce platforms.

These include Internet infrastructure risk, which my colleague Jeff Friedberg will be able to explain much better than I can because typically I'm turning to him to

understand what they're doing. Sales platform risks, obviously best illustrated by the highly publicized data compromises that are out there today. The risks continue - payment risks, best illustrated by the seemingly countless methods used by criminals to obtain fraudulent account information through phishing or pharming or other harvesting methods. And foreign government risks. My colleagues and I at the NCFTA believe that at least 80% of the criminals that are engaged in these schemes are outside the United States. How do we convince foreign governments to assist us when there are no victims, no loss, no concern. They only harbor the criminals themselves.

Relative to expanding the threat terrain, we have got a lot to look forward to over the next several years. As every financial institution requires more identity information to authenticate their users, we're in an information arms race with the criminals. As financial institutions require more, the criminals will steal more. Every report I read seems to point to more malicious attacks against the weakest leak in our chain, which is the consumer. And the computer that they sit behind, and I would imagine a cell phone as soon as we move to that technology to further commerce.

And this is going to be a very controversial point that I'm going to make. A couple of weeks ago I was in the UK. A serious organized crime agency invited me to participate in a meeting with the heads of information security for financial institutions in the United Kingdom. The underlying theme of the meeting was two factor authentication is not going to work. They have seen session hijacking as the wave of the future relative to compromise of these infrastructures and connections. Although it might not allow for extended identity theft, it would be very -- it will be very useful in good pump and dump scheme by one of the criminals for a short term attack.

I'm going to go back old school. I'm going to go back to an institution that I know and love, the Postal Service. And every day we visit over 150 million addresses, six days a week. How do we protect our citizens through the use of all of these technologies that we're talking about if we don't physically know where they are? And the infrastructure of the Postal Service provides a massive infrastructure for physical location. If 80% of the criminals are outside the United States, they don't have access to your mailbox in the front of your house.

So I have been working with a number of colleagues within the Postal Service to figure out how we can make this technology more useful for financial institutions and merchants and other organizations. We already rely on this technology. When I hear of an account data compromise, millions of credit card numbers compromised, that gives me job security because I know that the credit card companies have to reissue those credit cards and they're going to end up as revenue in that mailbox to fund my investigations.

We also provide an infrastructure for verification of transactions. If you change your address, financial institutions typically send a verification to a mailbox. Other types of account management transactions and other transactions could be relied upon by the Postal Service. The Postal Service could be relied upon for other types of transactions as well.

And we are working on a way for financial institutions and merchants to do verification of electronic transactions through first-class mail. And I'm joined today by some colleagues from the Postal Service, if they could just raise their hands, who are in our product development and postage technologies organization that are working to figure out how we can be a better partner for financial institutions to basically use that mailbox from a scanning perspective to confine risk to a geographic location. And assure that the remote transactions that financial institutions want to do with consumers are verified as to their physical location.

I'd like to thank you for your time this morning and I'd like to make a couple of comments relative to next steps. I think that there are four main points that I'd like to hit on relative to how we attack the criminals and work together with industry.

We need to understand and exchange intelligence from both government and industry relative to criminals that are trying to attack our financial infrastructure with identity information.

We also need to educate consumers and make them aware of the risks that are out there relative to the exchange of identity information, how to best protect it.

We need assistance from an enforcement perspective. My colleagues at the FBI, the Secret Service, Postal Inspection Service, we need all the assistance we can in order to go after the criminals and not necessarily be, at the end of the day, with an arrest, but at the end of the day come back with a tangible for financial institutions to be able to protect their infrastructures.

That gets to the last thing. How do we disrupt schemes? And that requires industry involvement and the involvement in government guiding industry into disruption of schemes. And in some cases, government has to guide financial institutions into disruption because the disruption is counter to the ease of use for consumers on financial applications. And thank you very much. (Applause.)

>>JEFFREY FRIEDBERG

I believe I'm the last speaker of the last panel, so it's my job to take us home. When Naomi originally asked me to join the panel she said, don't worry, you don't need to do slides or anything like that. Then I noticed my other two colleagues had posted some slide decks, and they're so colorful and wonderful, I got slide deck envy so I needed to put one together and I did it recently.

I think back in terms of the greater context that we're in. It's around this issue of reducing the pain of identity theft. I think also what Tom Kellerman said yesterday. He went through a whole list of horrible bad things that were happening to people, and I know a lot of us in this space who have been thinking about this have wrestled with, how

do you reconcile in your head all these different ways the bad guys are attacking systems?

And for myself, I really didn't have any choice but to create some kind of picture just so I could externalize and sleep at night. That ended up becoming this thing called the Internet battlefield which I have shared with a number of people in the room. I'm just going to show you a picture of it now so you can look at it. It's a little scary and it looks really complex. I normally take about an hour to go through this and I provide a nice tour. At the end of it most people walk away feeling enriched and aware of what's going on and also where maybe some of the tactics might go. But the purpose of the battlefield really is to demystify this very complex situation and to provide, hopefully, some insight into setting strategy and, furthermore, to assess the efficacy of tactics.

If I had to pick anyone -- just a very quick tour, the center line to the picture is phishing, the bottom half of the picture is really about deceptive software and spyware. All the lines connecting the two show you the complex way they interplay. There are also the things mapped out on here, including pharming, botnets, root kits, key stroke loggers, all different ways it is bad guys are using this data to abuse people, the role of law enforcement, et cetera. If I had to suggest a single take away from the picture, it's that the bad guys are constantly evolving their tactics.

I started this picture about three years ago. I have added to it over the years. It doesn't actually include some of the things like man-in-the middle attacks which are very common now. But just in terms of the picture, everything in red is a bad guy, everything in green is a good guy. In the center is the consumer in blue. It shows all the different ways that these actors play against each other. Bottom line is, there is no one solution that solves this picture. People come up with solutions and you can map them out on this picture and you'll say oh, look, bad guys can go around the side easily. So if you spend billions of dollars trying to solve one little element of the picture, that may not have been the best choice. So it's a good acid test.

Now, like many who have tried to wrestle with this, at Microsoft we thought it was a pretty important problem so we, a couple of years ago, kick-started an ID theft working group. After looking at this long and hard we came out with a bunch of key themes I want to share with you.

One of them, really top on the list, is this knowing who's who problem. I think we all agree that that is fundamental, hence the purpose of the workshop. But a key subtext to that is the need for enabling strong mutual authentication. I want to re-stress the mutual here. People earlier talked about this yesterday. But it's not just a bank knowing who the customer is. It's largely now the customer needing to know that it's really the bank. It's primarily because we continue to use what we call symmetric keys or shared secrets, user names and passwords, which if the bad guys can intercept, they can replay and pretend to be you. So that's the fundamental root motivation for phishing.

This leads us to the next theme which is, really, don't share secrets. If you can move to a different scheme where you're not using shared secrets it's going to help. So there are these things called asymmetric keys, or public private key pairs, and if we could actually deploy such a thing in a wide way it would actually leave the bad guys empty handed. There'd be nothing for them to phish because your public key is out there, everybody can get it, including the bad guy, and it doesn't hurt you.

That doesn't completely solve the problem because, in the back end, we have the data custodians and, unfortunately, there's been a huge number of breaches over the years, and now we hear about them, and it kind of gives us a real good sense of how big this problem is. In the back end, it's really about this comprehensive data governance need, where they're plugging the holes basically that might be there, but you have to also address things like insider attacks. And that really is more around auditing and reporting or other techniques, like role-based access, which we didn't actually talk about directly, but it's a key element to the big ecosystem of how to address this.

Now, of course, we're not going to get everything taken care of, so at some point law enforcement wants to come in and try to find these guys, but the bad guys are using a strategy called spread the pain. They hit people up for small amounts of money across multiple jurisdictions, just under the threshold for local law enforcement to take action. The strategy there really is around aggregation of crime so we could see the patterns and make it easier for them -- the law enforcement people -- to find and go after them.

And then lastly there's sort of this lend a hand. There are going to be victims out there and the more we can do to help them both contain the damage and clean up, it would be helpful. Here in the states we have Social Security numbers, but it's really not that easy to revoke one once it's been compromised. And the new account fraud or people that completely take over your identity, it's a gift that keeps on giving. It happens for years after. They continue to try to use those same credentials over and over again.

So in the years that we've been looking at this, has any progress been made? And I'm happy to report that yes, there actually has been some progress. First and foremost, I think there's general mutual agreement that mutual authentication, better mutual authentication, could really help here. I know the FSTC had a whole workshop on this. I currently co-chair one of the Better Business Bureau and ANSI panel on authentication. There was an authentication summit just last week. So in general, people are seeing this as one of the root causes that if we looked at it and kind of worked on it, might be able to make a dent.

The other thing is that there are better tools out there right now. It's easier to spot bad sites. In particular there are these new phishing filters and things like that, that use block lists and other heuristics to warn you. It's also easier to spot good sites. I know that Phillip Hallam-Baker mentioned the extended verification certificates. So just by looking for this sort of green bar within the browsers you might be able to spot that a higher test was being done for verifying the site. Also people have been using things like visual secrets that were mentioned earlier. When you go to your bank site, your bank

suggests you pick some picture that's unique that you can recognize and these are displayed to you so you can have higher confidence you're back at the right site when you revisit.

It's also less likely to get owned. I mean one of the biggest problems about all of this is that any time when your system can get compromised, all bets are off. So all these other tools really don't make any difference if your system's been compromised with some kind of spyware or root kit or bot or things of that nature. I know with the release of Vista we have this feature called user account control, which basically by default everyone runs at a lower privilege level. Why is this important? Older systems, most of you may still have in the house, a lot of people are administrator by default. If you have kids, things like that, well, guess what? If they go surf the sites, and they pick up some bad piece of software, that software gets to run with full privileges and it could wipe out your disc. Clearly, if you could run at, what we call, limited user levels, this is a fundamental huge benefit protection that you should execute on.

I know in my home I went to this model where all my kids were a limited user because I have been spiked with spyware. Ever since I went to that model, although it wasn't that convenient, I know I didn't get any spyware again for about a year and a half. So it really does help. Now we have automated ways where that can happen. There's also a new version of Internet Explorer that has a low lights mode that runs everything in a lower privilege until it really needs to do something special.

And finally, the breaches that we hear about, lost laptops hopefully won't be as big a deal if people use features where there's some kind of encryption. I know that we recently released this thing called BitLocker which does full volume encryption at the hardware level so there's really no excuse not to have this thing on.

To give you a visual here, this is the phishing filter working in the Internet Explorer 7, and any time that it detects a known phishing site, the entire address bar turns red and instead of seeing the site you're traveling to, this big flash page shows up saying warning, warning, you're at a phishing site. We have done a lot of tests on this and it turns out to be effective. When people see this kind of screen that says don't go, sort of the negative security model, people actually agree and don't go. They stop surfing. Since we released it, there've been over 34 million times that this was displayed to people, meaning that it gave them the opportunity not to go to a site that was an actually known phishing site. So this does really help.

On the EV certificates, this is what it looks like. There's a green bar at the top. As Phillip mentioned earlier, on the right hand side of the green bar it shows you the name of the organization in simple English, not the funny URL on the left, and in brackets it tells you where it is. So clearly if I saw a PayPal in Croatia, probably not the right site. It also tells you the name of the certificate authority. All of this used to be buried in the user experience, almost impossible to find unless you're an expert. This is helpful, and now it's available at a higher level. When we were testing, most people kind of got the impression that green meant go and that it was okay to proceed.

Also mentioned yesterday by Paul Trevithick was this thing called CardSpace. What you're seeing here is actually a card selector for this new identity metasystem that we discussed. It's a whole new paradigm. A way where you have this user centric identity people were talking about. And, unfortunately, I don't have time to go over this. In fact, one of my colleagues is running a breakout session after this where he's going to go into great detail and I highly advocate that people make use of that because this is something that's going to be very important moving forward.

This is how we get away from using names and passwords as just a simple user paradigm. In a short summary: the whole thing about CardSpace is, number one, its user centric. It puts users in control. All the data that is going some place goes through you first. You get to inspect it. You get to know what people are wanting to see and you can decide whether you want that to happen.

Next, it reduces dependency on passwords because under the covers it actually uses these cool asymmetric keys that everyone is talking about. Now I personally think that PKI and private keys and things like that are challenging for people to understand and hard to manage. This puts it a level below where people actually don't realize it's happening. I think that's how adoption really is going to happen.

It's also agnostic in terms of how it's been built. It uses open standards, the web services standards, which means anyone can build this. I know that we have seen java implementations and other things like that in the open source community.

And it also introduces something pretty important. It has a special ceremony. The whole screen kind of goes dark, this thing pops up, and you know you're doing something special. And to the degree that we can tell and encourage people to recognize that something important is happening about exchange of information, there's a better chance that people will have good habits.

And finally, it actually remembers relationships. It knows whether you have been visiting a site or not and can tell you that you're returning. This helps address pharming where you get hijacked in the middle of the DNS and you're not sure whether – even though you typed the right address, you end up being in the wrong place. That's e-pharming. This can help you detect stuff like that.

So other improvements that have been out there, in terms of seeing the crime patterns, I'm encouraged by the e-fraud network by the RSA. I think they have a bunch of banks working together with law enforcement where they're looking at suspicious transactions, where maybe it's a single computer, accessing many different accounts, or it's a single account being accessed from many computers. Both of those could be tip offs that it's fraudulent activity. I know that there has been a lot more law enforcement action since we started this project. I know Greg is responsible for some of those.

Also, there are some new services out there to reduce new account fraud. I know people talk about freezes and everything, but there's a company called Debix that uses a phone-based system that ensures that you get called before new credit is opened in your name. There are even stronger ways to go about this by putting a public key into your credit record. There are some ideas that have been thrown out there under consideration.

There are also smarter authentication methods that were discussed yesterday. I think risk-based is certainly more common. And it seems to be a good paradigm because you only get the appropriate speed bumps that are necessary for the value of the transaction.

And I have also started to see this thing called trusted favorites of directories, which is what we talked about a year ago, and I'll show you an example of that as well. On the risk-based authentication, when I went to pay my bill recently I did it first at work, then went home to check something. It immediately said, hey, you're using a different computer to log in. And I thought this was very interesting that it was recognizing that I was using a different PC. I think we heard also from Jeff Kopchik from the FDIC about using the computer as one of the factors. I thought this was a good example of that.

Now, with respect to trusted favorites, I know I can't keep track of my names and passwords today. I'm still waiting for PKI to roll out in great form, but I bought this little device, looks like a lock, it's actually a USB drive, and it's actually got a smart card in it so it can store my names and password for my financial institutions. I bought this at Target for $50 bucks. What you see on the screen on the left is a list of what they call my secure favorites. So what I do now is, instead of having to guess whether I'm traversing to the right place, again I'm evaluating this as an example of a new paradigm, I can click on one of these links and then it asks me for my PIN to access the secrets of my smart card. Then it proceeds to vector me directly to the site that I want to go to. Notice the green bar at the top. So this is an EV certificate showing me it truly is Charles Schwab, and that's all it was for me to do. I think things that make it easier for consumers to do the right things even with existing shared secrets, it's going to help.

So the question is, are we done? It seems like we did make some progress. Well, unfortunately, according to the stats, I know phishing is still going up. One number I heard is a 70% annual increase. And clearly there are more of these, what euphemistically we call downloaders, but it's what forms these botnets are getting installed. What's really scary is when you look and analyze these particular pieces of software, they're very sophisticated. The bad guy network advertises these things. They're called full featured crime ware. And they have every kind of different exploit just listed in a spec sheet, including screen scraping, et cetera. And they're ready to leverage exploits. Whenever a new hole is found in any of the systems, within 24 hours they're able to redeploy this particular technique out in the field. It's very scary.

Also we heard new technologies are certainly ripe for exploiting wireless in general, everything from BlueJacking or Bluetooth to evil twins at Starbucks where you have two axis points that look like Star bucks, but isn't. It's misspelled.

Or the voice-over-IP challenges we heard earlier. I know it was mentioned once or twice about medical, but it is a new type of fraud growing in terms of medical services. I know that in Queens, New York they recently went to a smart card based authentication system in order to know whether or not the patients are who they say they are. What's particularly challenging about medical fraud is that, to the extent that someone does get services in your name, now they're co-mingling your actual medical record with theirs and now it could be a life or death situation, not just financial. Very, very dangerous.

But at the end of the day I go back to that root theme we talked about, knowing who is who is absolutely fundamental to all these issues, including loading the right software from people you trust and lowering dependency on shared secrets is very important.

So what are some of these key challenges still left for us? I know one of the things that's particularly perplexing is what I call the trust experience. This is when you, as a user, are sitting down in front of your computer and you're propositioned to make a decision about something and you're not exactly sure whether something is safe or not. In addition, the way that the people at the other end are challenging you is all different.

For example, this little tool which shoves in user names and passwords, unfortunately, doesn't work when the financial site chooses to break up those questions across multiple pages. For example, I got to one site that asked me for my user name on one page, separate page asked for password and asked me for a challenge question at the same time. That broke this. So the problem is that we don't have any standards yet for the paradigm of how do you get challenged for these things and what to expect. That prevents people from innovating because it's still kind of all different.

In addition, these multiple cues that people are being provided means that none of us can really focus on a trust model. Someone mentioned yesterday about the need to have these mental models of how things work. They're constantly changing. So every time I see a little different kind of question I get challenged. I don't know whether it's an evil person or a real person asking these things. So we still have a ways to go.

And when I talked about the PIN that has to be entered for this, unfortunately, it's a virtual key board and those kinds of things could potentially be scraped by pad software if I had them in my system. The other thing that's a little disheartening is there've been a couple of really good studies done on the efficacy of some of these security indicators. One of them I'll mention to you is the visual secrets. I said that you pick a picture that's special to you and then it's presented to you each time you revisit. It turns out that at MIT and Harvard they did a study where instead of putting up the visual secret, they put up a little blank thing that said we're upgrading our system, our world class system, we'll be back in 24 hours. And guess what? Out of the 25 people tested, 23 clicked through

and provided their credentials. So this has to go back to the habits that people need to have and they need to stick with them. These methods only work if people use them.

Another example is even that green bar with the extended verification certificates. There's a study from Stanford and Microsoft research where they tested picture in picture attacks, and here is an example of what I mean. The window -- the outside window is the browser, and notice it's white on top. That means it's not EV certified -- in fact it says papal.login.com/ and inside the window is one that says paypal.com in green, but that's just a picture of that screen, it isn't the real screen. This is called a picture in picture attack. A lot of people have a real hard time telling the difference between the top address bar, which is the one you need to look at very carefully, and the pixels inside the window which you can't trust. Very, very challenging.

And it goes back to this issue that we still have a lot of research to do. We need to find these paradigms where people understand what are the trusted pixels? And quite frankly it's a very hard problem. We see this example of picture in picture attacks a lot, and it's one of the challenges that we all face when we come up with things that we think are going to be perfect. Well, no, there's work still to be done here.

One other point I want to make is around this issue of needing to be flexible. People call it diversity, et cetera, lots of different methods. When I got challenged by my bank that I was on a different computer, it offered me three different methods that I could use to prove who I was. I really liked that concept because, quite frankly, I don't always remember my secrets and I don't always have my tokens with me and things of that nature. I think the real challenge here is that in real people's lifestyles they're going to have lots of different devices with them and they may not be all the ones that the particular site expected. So having flexibility in what I'll call the authentication platform that other people brought up earlier is critical.

So the take aways. First off, there is still lots more to do as I pointed out. I think our collective vision, if I had to offer one, would be trust at a glance. We don't have time to look carefully at lots of written documents. We just need to know that we look at it, looks right, feels right, the ceremony is there. I have high confidence without a lot of work.

Next is, I think we really do need to match the user lifestyle. And I want to offer up this term -- personalized authentication. This is where, as a user, I get to choose which methods I can use based on what I have. And it's got to be of course based on risk. The backend system says the kind of transaction you want has risk X. The platform basically says I understand this person has these devices available. It's this combination that's necessary to meet the risk level. And you need this kind of flexibility in order for people to have this huge variety of ways they're going to represent who they are.

And of course, finally, we really do have to work together on this. It's a huge undertaking. Partially we're talking about infrastructure, so there's industry. There's of course all the research I have already mentioned that's been valuable. The work that law

enforcement is doing is being able to still allow law enforcement to get what they need done in terms of finding the bad guys, touching base with consumer groups, regulators, legislators. So again I'm very excited we're here trying to work on this problem, it's just there's still more work to do. But thank you very much. (Applause.)

>>NAOMI LEFKOVITZ

Thank you. This is the part where we're going to try to get this interactive discussion going. Of course, if you have questions, feel free to pose them, but not only the panelists can answer them, but other people in the room. So that's the idea here.

But I'll start by throwing out some ideas. We've heard -- I mean, last night I was thinking about this. Sometimes I never even know how to get into this problem because it's like my little son's whack-a-mole game where you whack down one thing, you think you got that conquered, and the other mole pops up. You know, if we spend a lot of money to create some great PKI system, then there's session scraping and there's work arounds and why did we spend all that money.

But let me just step back one second because we heard a lot yesterday about, we're not trying to reach perfection, and today we hear the market's not working. I'll put out something that we sometimes talk about in staff. Maybe the market is working. It's just working as well as it's going to because, as we heard yesterday, there's sort of this magic number of the 2% fraud rate. And so that's what businesses -- if it gets above that, then businesses are going to take action on their own and maybe that's sort of what was driving the FFIEC guidance is to say, you know, that's not good enough. And I don't want to debate here what the line is. It's not perfection, but evidently somewhere between perfection and 2% are several million consumers. (Laughter.) And victims. So that's what we're talking about. So let's keep that in mind.

And to that end, we wouldn't be here if we weren't talking about that space. So what do we do to drive that down? And is it government? Is it sort of an FFIEC regulation so it's sort of on the backs of industry? You got to spend whatever you got to spend to get it down somehow. Or can government help make this technology feasible? And would that be through the government purchasing power in purchasing technologies? And I'm just going to start throwing out practical thoughts. Is that HSPD-12? Is that mass purchasing of PKI and that technology? Are the smart cards going to help bring down the costs enough to make it feasible for businesses to use? Is the Post Office a good place -- can consumers trust it? Can they be a PKI issuer -- smart card issuer? They know the physical location. Let me start throwing some of those out there. You can start with panelists or if people have any ideas. We have got an idea back there.

>>AUDIENCE MEMBER

It wasn't an idea. It was a question of the panel. It's particularly the Microsoft representative. I know there are threats being described, multiple types of threats. As you said you can pound one down, another one pops up. One panelist mentioned if you

get compromised by one, even though you spent millions on solving another, you've got a problem. A pretty big problem. I know in USA Today there was an article yesterday about some compromises that were made of various software, Microsoft. To what extent do governments and institutions become the perpetrators? I know in the article yesterday it was the Chinese institutions that were involved. I'm just wondering if this is a new evolving threat area that is heavily financed or more financed than the existing sort of hacker community.

>>JEFFREY FRIEDBERG

Unfortunately, I didn't get a chance to actually read that article being here at the workshop. If you could describe it to me I could maybe better answer the question in terms of, is this something that you're thinking is new? Again I would need to evaluate it to let you know.

>>AUDIENCE MEMBER

Well, it might be a good idea to look at it, but I think in general it was an exploit where people from another country were getting into the utility software that's used generally on most people's computers like Microsoft Office and things of that nature. And getting into the machine to the extent where they became the trusted party in parallel with the operation that was going on the computer by the actual person so that there were concurrent sessions going on –

>>JEFFREY FRIEDBERG

Any time that, I said earlier, if you get owned, all bets are off. So any time someone can poke through any of your defenses, you have a serious issue of the integrity of the system. So one of the big considerations that we always tell people to use this thing called automatic updating because we're constantly vigilant looking for these kinds of issues that come up and we create these fixes. And if people don't have this automatic updating turned on they might miss the fixes and be exposed.

As I said earlier, within 24 hours or sometimes even shorter, amazingly bad guys are able to exploit holes. So it's this constant need to be on top of it, to have the best defenses you possibly can. I know within the company we also have this proactive thing we do called SDL, security development life cycle. I was struck by earlier comments about companies that don't apparently think security is important enough to make it a value. It's a core value in our company. It's something that the developers will go through from the moment they have a design on a napkin through the point of all the different release phases. And you can't ship without a final security review. So it's a very formal process that goes through.

These things certainly help a lot in terms of reducing likelihood of these things happening, but also point out that a lot of people, as pointed out earlier, don't reset passwords to other names. Defaults aren't always set, what I call weakened settings. So

it's still people's responsibility to some extent to make sure they have their defenses and their shields fully up.

>>NAOMI LEFKOVITZ

Can I interject for a second? We keep sliding, and it's natural to slide into phishing and fixing security holes. But isn't the reason that we're sliding into that because of this reliance on this sort of personally identifying information? Because that's what you can extract from people and databases.

>>JAMES LEWIS

Let me try that one because I wanted to pick up on your earlier remark, too. A lot of what we have been talking about are defensive measures. It's important. It's something we need to look at and talk about it, but we also need to think about what are the enabling measures. Particularly the concept of opportunity cost here. Which is, you have this technology, Internet and IT, and we are not making full use of it or we're making full use of it, and this gets to your market failure point, we're going towards making full use of it at a slower pace than we would if we had these enabling measures, like better identity management, better authentication. There's some neat stuff you can do with Internet technologies, in terms of buying, in terms of what consumers could do.

One example would be, suppose you wanted to go out and negotiate. Suppose instead of you going out and trying to contract through your natural gas, your electricity, you had a software agent that resided on your computer that would go out into the spot markets and buy for you. You would have a lower price. That's sort of a farfetched example, might sound like the Internet enabled refrigerator of a few years ago, but there are opportunities we're missing, and we're missing them because of poor authentication.

So one of the things we want to talk about is, how do we defend ourselves against attacks? The other thing we want to talk about is, how do we enable the next steps? I see Mike Nelson is raising his hand. Are you going to say Net 2.0?

>>AUDIENCE MEMBER

Mike Nelson with IBM. I just want to pick up on Jim's point and talk a little bit about the recurring theme of the last two days, which is interoperability. We tend to focus in these meetings on what it is the consumer does, what happens at the keyboard, what the smart card looks like. But there is half of the problem we haven't talked much about. That is, what happens in the back office systems and the storage systems. That is where a lot of compromises are actually happening. That is where the lost data tapes are ending up in the hands of hackers. There is a lot of need to focus on that piece as well.

And in that area we have got to do a better job of getting common standards, getting interoperable systems. I would like a little discussion about the barriers to interoperability. We haven't talked about what standards can do and need to do in this

area. We have got lots of examples where governments have pushed the wrong standard or they have actually been a barrier to standardization. You go back over the last 15 years, we had the European Union at one point decide it would only accept documents that were in Word. We have had government agencies that have only bought web authoring tools that only work with certain web browsers because they're not standard products. So as we go forward, governments have to be acutely aware of the standards their products support and they have to push industry together because our natural tendency is to go in lots of different directions.

Somebody gave the example earlier today where GSA had an interoperability lab. First thing they discovered is, none of the authentication systems worked together. It is not good enough for the vendor to tell you it works together. We have to find ways to make sure these products are working together at the user end and in the back office because that's where the most exciting new opportunities are going to happen. As Jim said, we have got this great new world of Web 2.0, new ways of putting software together, but that only happens if we have interoperable systems and that requires interoperable authentication.

>>JAMES LEWIS

Interoperable trustworthy systems.

>>JEFFREY FRIEDBERG

I would like to take that and respond to that. One of the problems with the Internet, I think most people understand, some people anyway, is that it was actually architected without an identity layer. So it was a fundamental gap in the way that it was developed. This is why you can be a dog on the Internet. To fill the gap people came up with different solutions over the years. There's things like X 509 certificates, Kerberos SAML tokens. There are lots of different ways to represent claims that people make.

The observation here is, let's say you have to pick one of these, and make sure you're betting on the right horse, make sure it's not the beta versus the VHS situation. It's a huge challenge. Which one do you pick? So this was sort of -- is one of the catalysts for what is called this identity metasystem, a system of systems, because you don't want to ever have to pick the right one. There's an abstraction being done at a higher level.

If you stick at any metasystem level, you can plug in all these different kinds of systems today, hence trying to drive this interoperability. This is why a lot of people are very enamored by some of the proposals like CardSpace and InfoCard and things like that. When you have this huge ecosystem where you have somebody who's vouching for you who is an identity provider and you've got some underlying partner like a merchant, God knows what systems are actually running. They have to talk common languages. So I think this whole movement towards an identity metasystem is a really good one for us. I encourage everyone to spend time at the breakout session to hear more about it.

>>AUDIENCE MEMBER

First off, I think you're absolutely right with the metasystems. I want to hit on the interoperability in a second. I'm with the Department of Defense Access Card Office. The interoperability is a huge deal. We're definitely working on that.

You asked the question originally, what government's role is. First off, to me it's very clear that government regulation and rules and laws can never keep up with the transient and the changing nature of a lot of the problems. First thing they can do, however, is start putting together dynamic rules and laws. For example, FISMA says it has to be compatible with or equal with whatever the current standard is. So many times we're looking at laws and regulations that say a particular point in time, and by the time it's implemented it's long past. How long has it taken to get the Real ID rule? By the way, you're not the only one in the room that actually likes that.

There are answers and I think we have heard all this. One of the common themes has been that there is no one solution. You have to take all the solutions together and pieces and where they're appropriate. For example, Department of Defense has integrated or started using cryptographic log on. We have seen in one year a 50% decrease in successful attacks. That is where HSPD-12 is going. Does it solve the problem? No, but it's a big part of it.

The other thing is technology is probably like 10% to 20% of the issue. Far more of this is the right policies, the right processes, and the right procedures, and are we using them? For example, one of the big things with cards and HSPD-12 that nobody is really looking at yet -- or there are two pieces. Number one is the pre-issuance specification. What does it take to get a card in the hand of the person and have it be secure? That's a 50 page to 100 page document that we took years to develop. And if you're not doing it correctly your security has gone out the window. You have no trust model in that system whatsoever.

The next thing is, somebody was talking about this yesterday, configuration management. Where am I today? Where am I going tomorrow? And how do I account for where I was yesterday? Once I have built this system, now what? How do I progress? How do I keep it going and how do I make sure it will still interoperate, which is what you were talking about. That is a huge, huge issue, because you're talking about the GSA lab. They can't read our card. We had to give them our own reader to read our card because -- part of it is also we already have a system out there and actually DOD will probably be the last one to implement HSPD-12 because we were the closest at the start. Sounds kind of counterintuitive, but it's true.

But to me it is going to be far more reliant in terms of progress, in terms of how do we make this, instead of a compliance issue for private sector, how do we make this a profit center? How do we make this something they want to move to, to be more -- hey, I can say I take better care of your information. I don't sell it. I don't trade it. I'm going

to protect your information. You should come shop with me. I think that's going to be something that's going to get people moving forward into it because, as we've heard, it has to be convenient and has to be something that the consumer wants to grab for.

>>NAOMI LEFKOVITZ

Take Avivah then Phil and then come back.

>>AUDIENCE MEMBER

I think we personally may be talking about the wrong issues. I think the role of government is to create skin in the game. So if you look at where consumers are losing money, it's not at the banks right now very much. They have done a good job of shifting liability and also protecting their own assets. It's with these unconventional attacks, like lottery sweep stakes, and between businesses. The Internet is everywhere. It's in printers, gas pumps, we're never going to get a handle on it. I think that the market will take care of solutions if government creates financial incentives and regulates the right things.

So what do I mean? Like make it easier for consumers to get their money back when they didn't lose it to a bank. Maybe they lost it to some fake spoof site and they have no clue how to get their money back. They used Western Union to transfer it. They may have used PayPal or other non-conventional money schemes where it's hard for them to recover.

Also, why doesn't government look at regulating all these information brokers out there? We can all get everyone's Social Security number on Google searches. Why is that happening? So if government creates incentives, I think the market will take care of itself. It will be technology solutions that will protect people because they don't want to sit there and pay consumers back when they lose money. In my view that would be the right question for this group to address.

>>GREG CRABB

Could I speak to that just for a moment? I think that there have been a couple of really good points that have been brought up. One is yours relative to the reliance of information generally. When the Internet was created -- I'm buddies with Steve Crocker, who was one of the researchers at UCLA that put the first note on, and he said we designed a system to share information. We're all here trying to come up with systems on how to stop the sharing of information.

When I sit down with some large banks in the United States, their biggest fear today is encryption isn't going to be able to be a technology that we can rely upon five years from now. How are we going to manage customer experience without encryption? I know criminal organizations -- and, you know, it might go well beyond criminal organizations -- are trying to defeat encryption. And we need to figure out

methodologies that we're going to rely upon in order to establish accountability for financial transactions and hold people responsible and allow financial institutions to do business. It's a big problem.

And then criminal organizations don't steal information just to have it. They steal information to conduct financial schemes and they traverse our channels that financial institutions look at, and from a consumer perspective, whether it's the banking, whether it's telephone or the Internet or the in-person methodologies that financial institutions use to interact with the consumer. Well, you know, the whole move towards mobile payments scares me to death. Because that -- in the context of what I know the threat environment to be, is scary. It's a dance around all these issues that it's going to take a lot more people than are around the table to be able to solve it. There's going to be some societal issues that need to be worked out relative to, is your data who you are, and, you know, all of those issues when it comes to authenticating to your financial institution.

>>NAOMI LEFKOVITZ

I think you have been waiting. Come back to Tom.

>>AUDIENCE MEMBER

Phil Hallam-Baker. Just to go back to the first question that was asked about government involvement and so on. Certainly information warfare is not a theoretical exercise. I have reports across my desk every morning. Clearly somebody is paying for gathering intelligence on terrorist groups using the web. Clearly we have a customer there or else it wouldn't be operational for us.

And the other thing here is that the U.S. has Fort Mead. Other governments have their Fort Mead. Just as everybody spies on everybody else, there are people spying on the U.S. Your other problem, though, is terrorists use non-government tactics and they may be more serious. In that one of the things that happens whenever there's an international crisis now is you have hackers on both sides piling on. One of the big fears is that maybe some of these hacker groups may cause a crisis to escalate when the diplomats are trying to de-escalate.

The other final point is money. The thing that differentiates a terrorist from a terrorist organization is money. The [inaudible] robbed banks and terrorized West Germany for 10 years; IRA protection rackets, kneecapping; Al-Qaeda, essentially they have Bin Laden's inheritance and once that was spent, they're basically drug peddlers.

If you're not careful the next generation of terrorists are going to be using the Internet and Internet fraud as their funds-raising mechanism. That's a government interest that says that government has a stake here and that it's not okay for banks and businesses to just throw their money at criminals who can become terrorists. If you look at the big organized crime groups -- the triads, the Mafia -- almost all of them have their

roots in some irredentist movement. So this is a serious, a national security angle here, and it's not being scare mongering to raise it.

>>NAOMI LEFKOVITZ

I'm going to let John, and then I think there's some others that have been waiting.

>>AUDIENCE MEMBER

Gregory, I asked Steve Crocker to try to attend today because I have always argued with him that the initial design of the Internet, while providing nice identification of devices and domains, ignored people. And it's one of the critical challenges. Now it seems absolutely opportune that you are here because we take for granted how valuable the individual address is. The guaranteed delivery of mail is the foundation for our entire super structure of commercial activities. Uniform commercial code relies upon the address for the delivery of a contract offerer. A revocation of a contract and on and on and on.

For you personally, maybe for others on the table, can we talk about guaranteed secure e-mail delivery? It seems to be one of the prototypical services we should be looking for in the future that may help us flesh out not only organizational framework, but the way to get there.

>>GREG CRABB

That's a huge project, John. Guaranteed secure e-mail. We've had a lot of conversations in the Postal Service. I have participated in meetings that have gone around and around on that topic for years. And I think a lot of people are happy with what they have today. Is Yahoo or AOL your e-mail of choice? And if you get what you want, you know, that's good. I think that there's a lot of business need for guaranteed mail. If you receive an e-mail message from your financial institution today, do you really trust it? We have a whole infrastructure that's missing because we can't rely upon the e-mail that we receive. And it takes into account a lot of different factors.

How do we assure that design of the Internet today is such that it's so dispersed that -- is it 90% of e-mail communications today are Spam? That's a major problem. How do we get authenticated e-mail? How do we do that infrastructure? There are projects that the Postal Service is working on around electronic post marking. We're talking to Steve and many others around how we do those types of technologies. But we need more of a business driver need in order to deliver that as a government infrastructure. Is it a government infrastructure like we have with the U.S. Postal Service? Is it a private industry infrastructure that's more focused on consumer needs? Those are huge barriers that need to be built and be spanned in order to be able to get to our end game of secure e-mail.

>>NAOMI LEFKOVITZ

I'm going to pull us back for one moment to some of the earlier themes and I wanted to pick up on something Jim was referencing. I think it picks up on some themes that Simon and Gus raised in the first panel. If identify theft isn't enough to drive a new system in the minds of the public and citizens, and I hear -- the reason I'm saying this is because I keep hearing about this interest in consumer, consumer-driven, consumer-friendly, consumer desire. And Jim started to say, are there other benefits that can be obtained that can be provided to citizens so that we can both reduce identity theft, yet these other benefits are so desirable, that they could altogether drive forward the will, the political will to build a better infrastructure, to allow some of these better technologies to flourish?

>>AUDIENCE MEMBER

My name is Perry (inaudible) with Verisign. One of the issues is that, and this reiterates something that Michael said from IBM, the vast majority of identity theft is because of data breaches and data mining, not authentication failures. So if I have a two factor authentication or a fob or a PKI certificate that I use to authenticate to my bank, it doesn't keep my identity any more secure because it can be lost by a waiter swiping my credit card at a restaurant or using my credit card at TJX. And that's one of the fundamental problems.

Identity theft is a big problem for consumers, but organizations don't -- it's not a big problem for organizations. Fraud loss is a big problem -- well, not a big problem, it's a problem for organizations because they take the hit. Fraud loss is not a problem for consumers. I don't care necessarily if someone uses my credit card or steals money from my bank account because I'm protected so I don't have any motivation to use stronger authentication if it's going to inconvenience me.

My bank or TJX -- TJX may be a bad example because they actually are paying a lot of money, but BJ's Wholesale Club years ago who lost lots of people's information and people were victims of identity theft -- it was just a cost of doing business to them. But the people who lost their identities went through hell to get their credit back. And so there's a fundamental problem of priorities with individuals and organizations. They just don't match. That's one of the reasons why this doesn't work.

>>NAOMI LEFKOVITZ

I think that, you know, that's an interesting point because when we were -- the staff was sort of brainstorming and we were thinking, what are some of the obstacles that we need to overcome? One of them seemed to us to be this sort of alignment of consumer behavior and the incentives of businesses. And do you have -- anybody have any thoughts on how to get those back in alignment? I'm going to take Gail and then Fred.

>>AUDIENCE MEMBER

I think it's going to be extremely hard for the -- Gail Hillebrand, Consumer's Union -- for the market acting by itself to set the bar in the right place for a very rational reason: businesses spread that loss over all of its customers. It's a small amount per customer. For the individual who is in that X percent, maybe it's the 2%, they're suffering that loss themselves, at least the inconvenience loss, the stress loss, the family emotional incidence. Maybe they'll get their money back, depending on how the money was stolen and where stolen from. I agree with Avivah that loss allocation and internalizing those risks by putting them on the business is going to help change the technology investment equation, but I think even as you look at risk-based authentication you have to be really careful because you're not looking at just the risk is X. The risk is X to the business and Y to the customer. And sometimes if you talk just about risk-based authentication, you are just going to talk about evaluating the X risk and not the Y risk. You need to pick up on both of them.

And finally, I think in the payment space consumers have expectations that will not be met. Consumers think they have more protection than they do. I talk to financial writers all the time who think you have charge back on your debit card. We all know the statute doesn't give you that. As we move into mobile payments, there will be devices that can be tied to a credit card with excellent consumer protections, a debit card with reasonably decent consumer protections that your money goes away, but you can get it back, and to a prepaid account that if it's not linked in some way to a deposit account you have no REG-E, and I think there's a real role for the FTC to set those ground rules on the front end before the mechanisms become widespread.

>>NAOMI LEFKOVITZ

Fred and Tom, and I know you have been waiting a long time.

>>AUDIENCE MEMBER

Fred Schneider, Cornell. I want to amplify those comments and put it in a slightly different way. Your opening remarks, Naomi, were about the market and whether the market is working. And it's clear it's not and it's not working for two reasons. One is because cost to business is being externalized. When a person has to go through hell to get their identity back, that's a cost that should be borne elsewhere and the wrong person is paying. So there's an opportunity to normalize the way costs are addressed. And second, markets only work when the participants have good information and consumers don't have good information about the risks.

There are two kinds of risks. One risk is having your identity impersonated, the other risk is having your privacy linking. So I think the exploration of authentication and identification, while interesting from a technological point of view, and it's sure good for a lot of non-technologists to know about, it is maybe a good way to spend a day and a half. I think you missed the point completely. I think the way to fix the problem is to fix

the market and to put in place whatever regulations are needed to get the costs attributed to where they should be borne and to get information in the marketplace.

And if that happened, I won't be surprised if various industry groups go to stronger authentication mechanisms. The credit card companies will have a great incentive to have authentication instead of identifiers as your authentication because they'll be paying a good deal of the loss that now is borne elsewhere in the system. But that's more natural than imposing a solution. I think there's an inflection point and you're not looking at it, and Avivah was pointing to it and the attorney from Consumer Union is pointing at it, and that is the real opportunity for government to have leverage. It's not by thinking about technological solutions which are going to move far faster than the government can move even in the absence of attackers, which seem to move at the same speed as technology.

>>JAMES LEWIS

Can I make a quick point to follow-up on that, Naomi? I think that's right, basically. Governments create the conditions for markets to work -- for markets to work better. In this particular case, the case that we're talking about, it has to be minimal, light-weight regulatory approach. It has to be technology neutral. Blah blah blah, all the stuff we say.

But we have to address two fundamental issues that the government can only address, I think. And the first is liability, as we've heard. The second is trust. How do we create trust? How do we link the individual and the identity to the machine or to the software? If you're saying what does government need to do? Liability and trust.

>>NAOMI LEFKOVITZ

Can we follow-up on, how does the government create trust?

>>JEFFREY FRIEDBERG

I can tell you right now that one of the things that Fred brought up, which is really critical, which hasn't really been talked about I think enough in the conference is this issue of the privacy concern. That, as we go forward looking for stronger ways to authenticate and things of that nature, there's an unintended consequence possibly of this linking of behavior that you don't normally expect. And as Simon and Gus mentioned from day one, it's the citizen centric model that we're looking for, where people are aware of what's going on and the 5 Ds. And I think someone mentioned earlier about how the latest revision of some bill didn't have the word privacy in it at all. It was removed. So what does that tell you? It says that part of the role of government is to maintain this balance and it's not doing that apparently if we don't have these important considerations done at the same time.

>>NAOMI LEFKOVITZ

So at the risk of being chastised, I'm going to throw it right out there, chastised by my bosses, but you're all dancing around the issue. Are we taking the wrong approach when we sort of use each bill to sort of address privacy within that particular initiative? I mean, do we need comprehensive, sort of comprehensive and comprehensible, because isn't that part of the problem that we're talking about that consumers don't understand the intricacies of GLBA, they don't understand the intricacies of HIPAA, they don't understand the FCRA, they don't understand where the holes are so that they can protect themselves. Do we need something comprehensible?

>>JAMES LEWIS

Yeah, is the short answer, with the caveat that, learn from the European experience which, whatever they did, it probably wasn't right. We can talk about that more.

>>NAOMI LEFKOVITZ

I know we're running. I want to make sure –

>>AUDIENCE MEMBER

Thank you. Gerald Beuchelt from Sun Microsystems. I would like to come back to the issue of liability. I think liability might be one of the great drivers and one of the great tools that government has and could expand on in terms of driving, at least the private industry, towards a more privacy aware and more secure way of authenticating people.

I think we've seen that. You mentioned that -- I believe a couple of minutes ago -- you mentioned that, for instance, the difference between BJ's security breach is that BJ's, and now at TJ Max over the course of this year, the security breaches at TJ Max are already creating a much bigger problem for the company than they did create for BJ's Wholesale Club in the past. If we start to -- if government starts to work on making liability a bigger issue for those companies that experience security breaches, the companies will be incentivized to better their authentication and make sure that security and privacy is preserved.

One way of doing that might be through -- to go through a federated approach. Where not necessarily every shop, every participant in the market, every part of a company sets up their own identity information, but instead starts to trust certain other companies that specialize in actually providing identity. That kind of trust would grow naturally out of the market without the necessity of government stepping in. Government might be one player in this identity provider market, but there would certainly be other providers in that market that are emerging. We've seen that actually right now with a lot of the smaller companies we're dealing with. Because they're starting to get away from

trying to store too much data about their customers because it is becoming a great liability. So they're trying to get away from that.

>>NAOMI LEFKOVITZ

Tom?

>>AUDIENCE MEMBER

Just first a quick comment on privacy and identity. I think different identity regimes have different implications for privacy. There was a discussion by both Greg and Jeffrey about shared secrets. And one of the issues with shared secrets in an environment where information is available is that the secret you have to choose becomes more and more personal in order to defeat the fraudsters.

There's a very interesting study I recommend for folks to look at by Alessandro Acquisti from Cornell University, looking at the amount of information folks disclose in their Facebook accounts. A typical consumer might disclose information like their favorite books, the school they went to, their birthday, their SSN. It's amazing what people will disclose. You have to think about that so if you're relying on shared secrets, there's a privacy implication.

The other point I wanted to make related to another role government I think could have, which is promoting research in this area. One thing I have had experience working with in this field for a number of years is the incredible divergence of statistics and assessment of what the problems are. The more we can get a quantifiable assessment of risk, I think, can help people go forward. Just to make one point here, there was a statement made earlier that 90 to 95% of identity fraud is attributable to data breaches. I know from studies that my own company has done we have not seen any indication of that rate. That's just one example where I think we need to do more research.

>>AUDIENCE MEMBER

(inaudible) from Alchemy. I just want to shift focus a little bit here. this is kind of a follow on to what Fred said earlier. It strikes me that the focus of the workshop is on authentication technology solutions, as well we need to discuss. But I think we need to be careful that we're not chasing our tail with discussing solutions when we really don't have solid ground truth as to the nature or extent of the problem itself. In that regard I would just point to sort of the green elephant in the middle of the room, which is the failure of business to disclose the breach or fraud to begin with.

From a consumer side, consumers have to jump through many hoops in order to be made whole from the credit companies. They have got to file police reports and do all sorts of things. I think we need to talk about requiring business to, as a condition of underwriting their fraud losses, disclose the fraud incident data to begin with and then we can start to get a good feel for the aggregate nature and extent. This can be done in a

privacy preserving way. There's a layer of abstraction that this information can be shared and we can get a better understanding of the nature and extent of the problem and also get a better understanding of the nature and extent of the solutions -- these authentication solutions we're proposing here.

>>JEFFREY FRIEDBERG

So this is Jeff Freidberg. One of the other themes I didn't share with you is check the math. This really has to do with scrubbing the numbers. Since a lot of public policy is based on what the perceived statistics are, it's very critical that we have reasonable metrics that we understand what we're looking at. Different kinds of fraud, how it's happening.

There's a nomenclature problem all over the place. Originally people called breaches identity theft, for example, and a lot of people were running taking action based on information that may not be exactly what they think. So I totally back your recommendation that we also invest in that aspect. Because it will help all of us and I think it should be international also so that we actually can see the trends. So, great idea.

>>GREG CRABB

If I can just talk about trust for a moment. Naomi began the presentation, she indicated that the Postal Service is the most trusted government agency based on studies. If we were a corporation, we would be 21st in the Fortune 500. Our revenues are about $73 billion a year.

Now, how does an organization that size that has a public mandate that services everyone in the United States maintain trust? Well, first of all, except for a change of address system where we keep the records for one year, we don't associate any identity to the address that we service. We don't keep your name on file relative to the address where you live. So we disassociate identity.

We also have 1750 law enforcement officers that are dedicated to maintaining trust. And relative to disclosure of information to law enforcement, private industry could enhance their ability to establish trust among individuals if they provide information to law enforcement because the criminals that I put up on the screen, they're hiding within the percentages. And it's not 2%. Identity frauds are not 2% of most organizations. It's typically .1% of fraud for a particular organization. But that .1% represents billions of dollars of fraud that needs to be shared with a law enforcement entity. This is law enforcement by anomaly, I guess. And figuring out how we can develop better law enforcement systems to go after the criminals. And a lot of criminality can be committed by the billions of dollars that that little percentage represents.

>>NAOMI LEFKOVITZ

Yes. Am I missing anybody over here?

>>AUDIENCE MEMBER

Martin Bosworth, of My Public Info. I know we're running short on time so I'll just read to you a bit of a news item that my boss e-mailed me this morning. This just came in while we're here at this conference. Keep this in mind. Computer equipment containing the personal data of nearly 160,000 current and former employees of the Neiman Marcus group has been stolen. The equipment has been owned by a third party pension benefits paying consultant that has not been named. The stolen files contain data from 2005 including Social Security numbers and salary information. Now this just happened while we were here.

There are so many things that go wrong in that statement, I don't know even know where to start. First of all, the fact that they outsourced this information to a third party. When you open up your data chain, the more you open it up, the more weaknesses you're going to have. The human factor is the biggest weakness. The second part, would we have even known about this if there wasn't any incentive for data breach laws, if there wasn't any mandated notification for them? Of course not. They would have kept it completely hidden and we would never have heard about it. Anybody that could afford to shop at Neiman Marcus, I can't, but anyone who could might have suddenly had their credit cards used against them, their identities stolen. They would have never known why. All the expense would have been on them to fix for a crime that was never theirs to begin with.

We have talked extensively at this conference about authentication technologies, multi-factor authentication. All of this stuff is extremely important, extremely necessary, but none of that played in this scenario. It was somebody who misplaced a computer or left it in a car or left it in their house and it got stolen and they don't even – it's just ludicrous to me how these things are not better managed and not better monitored. And we can't let that opportunity to have this better enforced slide. You can't sit and say the market's going to take care of it because, left to its own devices, the market will not take care of it. There needs to be better enforcement on this level. I'll open this to anybody that wants to address it. I'm sorry for the speech.

>>JEFFREY FRIEDBERG

Just realize that we did discuss the, sort of, the plug-the-leak strategy which is very critical, which addresses some of the insider issues that can happen, the lost laptop, things of that nature. I think there is an awareness, at least by some companies, that they need this concept of a data governance strategy of how they manage all the data that they actually are responsible for. I also mentioned the auditing and reporting capability which is that, when things get abused, you know who had access last and you can track to it the individual person who you might need to go after. This all helps create the deterrence necessary to say, well, it's not a free lunch, it's not that easy to do. It is a step in the right direction.

>>JAMES LEWIS

Let me really quickly say the other thing you might want to think about is, what's the actual distribution of the cost here? When you look at the cost to a company as opposed to – we've all heard it's terrible for individuals, and it is. But for a company, it's a rounding error. Especially for some of your larger financial institutions. And why would they bother? This is not a big deal for them. So one of the reasons when you talk about who is going to make who do what, bear in mind, I have some data on this, it's a very tiny fraction of a percentage when it comes to the cost of Internet fraud for most of the big financial companies.

>>NAOMI LEFKOVITZ

One more question then I'm going to do a little wrap up.

>>BETSY BRODER

Looks like an inside job, right? You would think that at the end of this conference it certainly is a terrible thing that all of this data was lost. But maybe the point of conversation from that news is, isn't it a pity that people can still use the information that's stolen to commit fraud? Shouldn't the end game of our discussion here be, so what? You know, they got a bunch of random nine digit numbers. Shouldn't we be at a point in our discussion where that doesn't matter because we achieved a better form of authentication and if you will disincentivize the data thieves so they're not looking for the data any more because we have stronger ways to ensure that once it's stolen it can't be used.

>>NAOMI LEFKOVITZ

We didn't set this up, but it's a perfect segue because we have a few minutes left and I just want to talk about the action items that I have on my list. For government, I have fix the imbalance in the market. (Laughter.) And tomorrow -- and after that we're going to fix the liability problem. And we're going to create trust. Maybe we could – you know we posited that perhaps we need a more comprehensive, comprehensible privacy scheme.

On industry side, for action items I heard disclosure. I think I felt like a collective cringe on that. So are there other action items that industry could be taking?

>>JAMES LEWIS

Interoperability. Reliability.

>>NAOMI LEFKOVITZ

So you guys can work on that. All right. (Laughter.)

>>NAOMI LEFKOVITZ

And finally –

>>JEFFREY FRIEDBERG

I think ease of use was in there too.

>>NAOMI LEFKOVITZ

Ease of use. Great.

>>AUDIENCE MEMBER

Liability.

>>NAOMI LEFKOVITZ

Liability. And is there anything that we can expect from consumers? Or do we -- we do it all for them?

>>AUDIENCE MEMBER

Consumers have no choice (inaudible) sitting ducks (inaudible).

>>NAOMI LEFKOVITZ

Okay.

>>JEFFREY FRIEDBERG

I think the consumer one though was adopt good habits. It's kind of like buckle your seat belts.

>>NAOMI LEFKOVITZ

Responsibility.

>>AUDIENCE MEMBER

The first $50 is yours. That's tied right in to responsibility, tied right in to how we do that. Put some liability on the individual. I can lose my wallet. It isn't just a computer. But it's got to be –

>>JEFFREY FRIEDBERG

At the end of the day, even if I had asymmetric keys or the private key on a fob, if a friend comes over and says, can I borrow your fob and tell me your pin, don't do it. This won't protect you with that kind of issue. Good habits help.

>>NAOMI LEFKOVITZ

All right. Demand security. Thank you very much. This is going to conclude this panel. We are now going to have closing remarks from Lydia Parnes, Director of the Bureau of Consumer Protection.

>>LYDIA B. PARNES

Thanks Naomi. I spent most of yesterday doing a variety of briefings on the Identity Theft Task Force Strategic Plan that was released here in the afternoon. So, unfortunately, I missed this conference, but got to listen to a little bit of your discussion this morning and I have to say it sounds great. I'm sorry I missed it. I plan to watch the archived webcast because one of the things that we know is that we have to work together to resolve the issues that we're confronting. And you obviously are the right group of people to be addressing this issue because everybody is so engaged and already coming up with such excellent ideas.

As the Chairman mentioned yesterday in her opening remarks for this conference, this event actually lets us check off one of our must-dos for the task force. It's obviously a significant accomplishment because in the past day and a half, we heard from an extraordinarily distinguished set of panelists and moderators about the ways in which we can improve our authentication systems to help us reduce identity theft.

It's so obvious just listening to you these past few minutes that you all recognize the challenges that we face in building systems that will meet the needs of government, industry, and consumers. But I'm optimistic in listening to you that the information that you've all put forth and through the questions that have been asked during the workshop, all of this information will help us identify solutions to determine a person's identity and ensure that people, in fact, are who they purport to be.

So yesterday morning we began by examining the ways in which we structure authentication and identification systems and the need for buy-in from all of the stakeholders. The opening panel, Simon Davies and Gus Hosein talked about the necessity of five Ds, discourse, deliberation, decision, design and delivery -- these guys could work for us -- and how failing to take any one of these elements into account can greatly impact the successful launch of any identity system.

In light of these considerations, it's important to understand how identification initiatives currently under development meet or don't meet these objectives. While the original use of Social Security numbers was a very legitimate need to track workers'

earnings for benefit purposes, the expanded use of these numbers as a widely used identifier has rendered them the most valuable piece of information for an identity thief. We have to learn from that experience when we look at newly developed unique identifiers and consider how these new identifiers will be used in the future so we can ensure privacy and maintain security.

When the FTC staff first considered what would be the best focus for this workshop, given the breadth of the topic, authentication technology was an inevitable part of the discussion. But the folks putting this workshop together concluded that focusing exclusively on technology would not be as effective as examining how technology fits within the context of our policy goals. But of course, in order to understand that fit we have to understand how the technology operates.

So yesterday afternoon we heard about a broad range of technologies that can help us better authenticate individuals. One theme that emerged loud and clear was that no one technology will be a silver bullet. To have an effective strategy, we have to layer together different technologies and counter measures. And above all, we have to remember that if the consumer can't understand or use the technology, it simply won't be effective.

To that end, we learned about the importance of consumer education in introducing any new authentication system. Today we learned about some of the exciting ways technology is being used in other countries to provide consumers with even greater convenience in their daily lives -- ways that we're just beginning to explore in the United States. We learned about some of the challenges and risks that need to be addressed to ensure that this convenience doesn't come at a greater cost to our security and privacy. And in turn, we shared some of our experiences with developing an identity ecosystem that allows individuals to maintain their trust and privacy while increasing security through the use of diverse identifiers and credentials.

As Chairman Majoras noted in her opening remarks yesterday, this workshop is really a historic event; it's an important step forward in our fight against identity theft. Each of us, government, industry and actually even consumers, as we heard, we all have a role to play. Government can help lay the foundation for a healthy market by ensuring consumer trust and supporting an infrastructure within which technologies can flourish. Industry can work not just to develop and implement better technologies, but also to implement the practices, such as consumer education and employee training, that will let those technologies succeed. And consumers can understand the importance of layered security in protecting their welfare by not only cooperating in its deployment, but demanding it from industry and government.

I'd like to conclude by thanking everyone here for their participation. I also -- you know, our folks who put this together, I know they have been thanked, but they really did a spectacular job, Naomi, Joanna, Kristin, Stacey and Alicia. Can you all stand up? (Applause.) What a great job. And thank you so much for your hard work on that. I

hope you all enjoyed this past day and a half. Have a good lunch and come back this afternoon for breakout sessions. Thank you. (Applause.)