

>>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 that-- in the last day and a half that we would then sort of 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 we 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 remind-- 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 in this case there's many ways to reduce identity theft but in this case obviously through better identification and authentication. And-- 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 sort of put forward the objective as only on solving identity theft, that doesn't necessarily carry an identification system. Perhaps I'll put forward this thought, that that's because perhaps it's because 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 like Paul was saying about-- you know, 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 for the center for strategic international studies. We have George 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, chief privacy architect.

>>JAMES LEWIS

Thank you, Naomi and thank the FTC for invite Meg to speak. I'm glad to see the strategy. It's very help I. The last question was right on. I think we need to talk about the role of government. As we were discussing during the break you need both, government and private sector. 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's two central problems when I think about this, how do you-- 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 have heard yesterday. And untrustworthy environment. And another problem we need to pay attention to is how do we adopt what are basically paper processes that we have developed over the last Century to what are now digital and networked applicationsch 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 g through the slide. The main point I would like to call your attention to is that 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 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]

>>JAMES LEWIS

We have a lot of things going on in the authentication space. Right? And there's 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 a pseudo ANIMITY. We might have right now too much of that but we need to blend T. second thick you have heard consistently is trust is expensive and people don't want to pay for it. 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 scene we have heard before. We have what we call liability dodge ball. You know, 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. 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 would 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 people were used to horses and the horse was intelligent. If it says you it probably wouldn't bump in to you. So somebody walks in front of a car waving a red flag and so people would know a car was coming and wouldn't scare children. That's part of how we understand these problems. We ask ourselves what

are the problems I'm going to have the deal with? I have at an event a couple of months ago where someone said the real idea act was the first step towards an American GESTAPO. Unfortunately those attitudes are 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 let mess know how you-- lets me know how you are going to identify yourself? The key for me is how do you start networking these things? A problem in the U.S. that I don't think Japan or Norway has is we have a federal system so you have dozens of entities issues 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 t 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 into crease 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 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 would have is a brand name and even that I'm not sure about. What are the processes that lay behind your issuance for that-- you're issuing that credential? If I don't know those or have way to assess them, 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 assume it's relatively trustworthy, it's from someone else maybe I don't know. Some of the things we need to think about what are the rules for authentication? This includes what Naomi mentioned. We need rules for privacy. If people are uncomfortable that their privacy is being protected they won't play. We need rules for how you opt in or out. I would prefer an opt in system because that helps you deal with the objections. You're worried that real idea is the first step towards the GESTAPO, don't get one. That let leave mess free to move ahead. We need to think how to assign liability. Not an issue that we've resolved. Finally with need to think about enforcement. I think some of the things we saw in the strategy are helpful on the enforcement side. The question that we heard from NTIA was there's-- 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 a problem that the private sector nor the government can solve by themselves. So one thing 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 '96; 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 how do we accelerate better identity management, better authentication in the U.S. and elsewhere? Some is to assign responsibilities. Government-- responsibilities. Government play ASCII role. I will like to come back to that. On the interoperability side government should not get into the stand cards business. Government should not dictate technologies. You can see this in other countries, Germany had a digital signature technology. If you say there's one technological solution, and we all must use it, that's not going

to work. The issue of rules who is boeing to set the rules for the identity system we have? It has to be plan. The government can do certain things, private sector can do certain things and they need to find a way to work together. What would be my next steps? If it's 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 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 using 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, used to be about 300 bucks now I think it's like 7 700 bucks now. But I can get you any driver's license you want. You want to be George bush or Osama bin lay den, just pick. So we need a better process how the government issues those crucial credentials at the beginning. We need to develop a way for the government and 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 about that earlier. If you don't have these privacy safeguards people won't use these things, at least in the US. 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 well, I myself am comfortable with it. It doesn't appear to be working. So some sort of standard who sets the standards? Some mix. Is it the banks, the credit card companies, is it the government? It's got to be a blend. And finally think about where we need legislation. Whether that's assigning liable, none of you worry about credit card fraud much because your liability is covered, right? You're only liable for 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 credentially rules we have are enough. Real ID which I might be the only person left on the planet who likes is useful step in

that direction. The fraud and privacy measures certainly the FTC strategy does a lot, that's the third time I said it, does a lot on the fraud side. You see other steps going along. On privacy, the larger debate 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 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 need to accommodate diversity. There's 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. It's not going to happen now. You need to think about how to promote interoperability. It 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 you can trust your credential. How do I know how trustworthy it is, how do I measure that trust in those are things we haven't 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 -- and by answering the question, government is an enabler, and a guider, but it's not going to be the normal role of government as marching to creating but smu creating and 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 want 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 that some information 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

>>GEORGE 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. I'm a Program Manager responsible for Cyber Crime investigations in the global investigation division. I'm going 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 vaitive intelligence-- investigative intelligence initiative with the FBI. 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 it tease national cyber forensic and training alliance we monitor sifts of thousands of cyber criminals engaged in account take overschemes, false application scheme shs identity theft, credit card fraud investigations, brokerage scheme, 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 beyond credit card fraud. Under the umbrella of

interpoll and with law enforcement from 30 countries we work under the operation name Operation Gold Phish, to-- to target cyber criminals around the world engaged in network sales, the activities have included a number of arrests in the yeern Europe, West Africa, European Union, and the Middle East. How many of you have seen the movie BORAT? Actual hi some people will admit to that. No.

[laughter]

>>GEORGE CRABB

In so many ways that movie is so wrong but in many ways it's an excellent portrayal of cultural-- culture and prejudice. The film seems like a somber exploitation of prejudice yet has men running naked through hotel hallways, drunken Fratt boirks street kids willing to provide some coolness tips, and so many other things that are just so wrong. But in the film BORAT refers to a trojan horse. But as the audience leaf it is theater wondering whose prejudice has been exposed, the question of where the real trojan horses is link gers as a fake anthem accompany it is 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 laugh out loud comedy, insiding an expose of the audience itself. As I left the movie alongside my analyst at the national training alliance and close colleague and 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, subtitle BORAT, the cultural learnings relative to our understanding of America on how these criminals make benefit of the glorious anarchy Cyber Crime. These criminals are making a mockery of the cultural tendencies of 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 publicly sized data compromises out there today. The risks continue. Payment risks best illustrated by the seamless countless methods used by criminals to obtain fraudulent account information through phishing or farming or other harvesting methods. And foreign government risks. My colleagues and I at the NCFTA believe that at least 80% of the criminals engaged in these schemes are outside the United States. How do we convince foreign governments to assist us when there's no victims, no loss, no concern. They only have-- they only harbor the criminals themselves. Relative to expanding 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 fringe of our chain which is the consumer. And the computer 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 they I'm going to make. A couple of weeks ago I was in the UK, the serious organized crime agency invited me to participate in a meeting with the heads of

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 connects. 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 criminal force 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 organizes. We rely on this technology. When I hear of a 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 could be relied upon b for other types of site transactions as well. And we are working on a way to-- 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 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 enforcement perspective. My colleagues at the FBI, secret service, postal Inspection Service, we need all the assistance we can to go after the criminals and not necessarily with 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 it's-- in some instances these -- 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 posted some slide decks and they're so colorful and wonderful I got slide deck envy so I needed to put one together I did it recently. I

think back in terms of the the greater context we're in. It's around the 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 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 ways the bad guys are attacking systems. And for myself, I really didn't have any choice but to create some kind of picture so I could externalize and sleep at night. That ended up becoming this thing called the Internet bat field which I have shared with a number of peep in the room. I'll show you a picture so you can look at it. It's a little scary and looks 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 is to demystify this very complex situation and to provide hopefully some insight into setting strategy and furthermore to discuss the efficacy of tactics. If I had to pick anyone-- just a very quick tour, the center line of the picture is phishing, the bottom half is about the software and spyware. All the lines connecting the two show you the complex way they interplay. There's also things mapped outen here including farming, bot nets, root kits, key stroke loggers, all different way 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 (indiscernible) which are 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, 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 element of the picture, that may not have been the best choice. So it's a good asset test. Now, like many who have tried to wrestle with this at Microsoft we thought it was an important problem so we couple of years ago kick started a ID theft working group. After look at this long and hard we came one 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 is fundamental hence the purpose of the workshop. But a key sub text to that is the need for enabling strong password actual authentication. I want to 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 yiewrser names passwords which the bad guys can enterrepresent, replay and pretend to be you. That's the fundamental route motivation for phishing. This leads us to the next theme which is don't share secrets. If you can move to daircht scheme where you near not using shared secrets it's going to help. So there's public private key pairs. If we could deploy such a thing in a wide way it would leave the bad guys unbehanded. There's nothing to phish because your public key is out there, everybody can get it, it does doesn't hurt you. That doesn't completely solve the problem because in the back end we have data custodians and there's been a huge number of breaches over the years, it gives us a sense of how big the problem is. In the back end it's about this comprehensive data government's need where they're plugging the holes basically that might be there but you have to also address insider attacks, more around auditing and reporting or other techniques like role play access which we didn't actually talk about directly but is a key element to the big ecosystem of how to address this. 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 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's going to be victims out there and the more we can do to help them contain the damage and clean up, it would be helpful. In the states we have Social Security numbers but it's in the that easy to revoke one once it's compromised. And the new account fraud or people that take over your identity, it happens for years after. They continue to try to use those same credentials over and over again. So in the years we have been looking at this has any progress been made? Yes, this 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 workshop on this. I currently co-chair one of the IDS better business bureau panel on authentication. There's an authentication summit last week. So in general people are seeing this as one of the root causes that if we looked at it and worked on it, might be able to make a dent. 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 things to warn you. It's easier to spot good sites. I know that Phillip and 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 to-- 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 a picture that's unique so you can recognize and these are displayed to you so you can have confidence you're back at the right site when you revisit. One of

the biggest problems about this is any time when you system can get compromised all bets are off. These other tools don't really make a difference in your system is compromised with a spyware or root kit or bod or things of that nature. I know with the release of vista we have account control which basically 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, if they go surf the sites, that software gets to run with full privileges and could wipe out your disc. Clearly if you could run 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 my kids were limited user because I have been spiked with spyware. Ever since I went to that model, although not that convenient, I know I dip get my spire ware again for about a year and a half. So it really does help. Now we have automated way force that can happen. Another a new version of Internet explorer that has runs everything in a lower privilege until it needs to do something special. The breaches we hear about, lost lap tops hopefully won't be as big a deal if people use features with some kind of encryption. I know we released bit locker which does encryption at the hardware level so there's not an excuse to not 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 dress bar turns red and instead of seeing the site you're travelling to, this splash page shows up saying warning you're at a phishing site. We have done a lot of tests on this and 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's been 3 or 4 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 help. On the 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 gripe bar it shows 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 papal in CROATIA, probably not the right site. All of this used to be buried in the user experience, almost impossible to find unless you're an expert. This is helpful and available at a higher level. Most people kind of got the impression that green meant go and that it was okay and to proceed. Also mentioned yesterday by Paul was this thing called hard space. An example of the-- this what you're seeing here is actually a card selector for this new identity system that we discussed. It's a 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-- unfortunately I don't have time to go over this, one of my colleagues is going to go into detail about it in the break out sessions. This is something very important moving forward. This is how we get away from using names and passwords as just a simple user paradigm. Short summary. The thing about card space is number one, user centric. It puts users in control, all the data that is going some place is going through you first, you get to decide whether you want that to happen. Next, reduces dependency on passwords. Under the covers it uncovers these asymmetric keys that everyone is talking about. It's challenging for people to understand and hard to manage. This puts it under a level below where people 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 built. Uses open standards. The-- standards. The web services standards which means anyone can build this. I know we have seen job implementations and things like that in the open source community. This thing pops up you know you're doing something special. And to the degree 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 relationship, know where is you have been visiting a site or not and can tell you that you're returning. This helps address arming where you get hijacked in the middle of the DN, is and you're not sure whether-- eet iryou typed the Wright address, you end up in a different place. That's farming. This detects things like that. In terms of crime pa terms I'm encouraged from the E fraud network by the RSA, boshing together with law enforcement 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 off it's fraudulent activity. I know that there's been a lot more law enforcement action since we started this project. I know Greg is responsible for some of those. There's new services throughout to reduce new account fraud. Know people talk about freezes but there's a company called die vex that uses a phone based system that ensures that you get called before you credit is opened in your name. They're even stronger ways to go about this by putting a pubkey into your credit record, ideas that have been thrown out there under consideration. There's also a smarter authentication methods 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 necessary for the value of the transaction. And I have also started to see this thing called trusted favorites of directory which is 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 prison very interesting it was recognizing that I was using a different PC. I think we heard from Jeff from the FTIC about using the computer as one of the factors. I thought this was a good example of that. Now, with respect to trust to favorites, I know I can keep track of my names approximate passwords today, I'm still waiting for PKI to role out in great form but I bought this device, looks

like lock, it's actually a USB drive that's got smart card in it so we can store my names and password force my financial institutions. I bought this at target for \$50. What you see is the list of 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 asked me for my pin to access the secrets of my smart card, then it proceeds to vector me directly to the site I want to go to. This is an EV certificate showing me it truly is Charles Schwab and that's all I need to do. It makes it easier for consumers to do the right things even with existing shared secrets it's going to helpch are we done? Seems like we made progress. Unfortunately turning to the stats I know phishing is still going up. One number I heard is 70% increase annually. There's downloaders but's what form these bot nets are getting installed. What's scary is when you 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 speck 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 about new technologies are certainly ripe for exploiting wireless in general, everything from blue Jacking or Bluetooth to evil twins at Starbucks where you have two axis points that hook like star bucks but isn't. Or the Voice-over-IP challenges we heard earlier. I know it was mentioned once or twice about medical but a new type of fraud is growing in terms of medical services. I know in New York they recently went to a smart card based authentication system to know whether or not the patients are who they say they are. Cha wha's particularly challenging about medical fraud is to the extent that someone does get services in your name, now they're co-mingling your medical record with

theirsnd 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 route theme we talked about, knowing who is who is fundamental to all these issues including loading the right software from people you trust and lowering shared secrets is very important. So what are some of these challenges 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 sure whether something is safe or not. In addition, the way that the people at the are challenging you are all different. For example this tool which shoves in user names an pass words 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 pass word and asked me for a challenged question at the same time. That broke this. So the problem is we don't have any standards yet for the paradigm of how do you get challenged for these things and what to expect. That keeps people from innovating because it's still kind of all different. In addition, these multiple queues that people are being provided means that none of us can really focus on a trust model. We can't-- 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 if 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, it's a virtual key board and this kind of thing could potentially be scraped by pad software if I had them in my system. Other thing dishart heartening, there's been couple of 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 presented to you each time you revisit. It turns out that at MI

tirks 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 provide 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, the green bar with the extended verification certificates. A study from Stanford and Microsoft research where they tested picture and 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, meaning not-- in fact it says papal log in.com and inside window is green. But that isn't the real screen. This is picture on picture attack. People have a hard time telling the difference between the top address bar and the pixels inside the window which you can't trust. Very, very challenging. And it goes back to this issue 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 very hard problem. We see this example of picture picture 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. 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 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 liked that concept because quite frankly I don't always remember my secrets or have my tokens with me. Things of that nature. I think the challenge here is that in real people's lifestyles they're going to have lots of devices with them and they may not be all the ones that the particular site expected. So having flexibility in what I call the authentication platform that other people brought up earlier is critical. So the take aways. First off, there's still 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. So the back end system says the kind of transaction you want has risk X. The platform basically says I understand this person has these devices available. This combination is 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. Finally we really do have to work together on this. It's a huge undertaking partially talking about infrastructure, so there's industry, there's all the research I have 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 group, regulator, legislators. So again I'm excited we're here trying to work on this problem, it's just still-- there's 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. I'm like sometimes I never even know how to get into this problem because it's like one of those my little sons ball game where you wack 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 or something, then there's session scrapings and work

arounds and why did we spend all that money. But let me just step back one second because we heard a lot about we're not trying to reach perfection and today here the market is not working. I'll put out something that we sometimes talk about. Maybe the market is 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 business-- 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 FFIAC guidance is to say, you know, that's not good enough. And I'm not going to debate-- 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]

>>NAOMI LEFKOVITZ

And victims. So that's what we're talking about. So let's keep that in mind. And to that end, so how do we, you know, 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 FFIC 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 in using that 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 to-- can Consumers trust it? Can they be a PKI issue-- smart card issuer? They know the physical location? Let's start throwing some of those out there. You can start with panelists or if people have any ideas. We have an idea back there.

>>MALE SPEAKER

It wasn't an idea. It was a question of the panel. It's particularly the Microsoft representative. I know there's threat 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. Pretty big problem. To what extent now, 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 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.

>>JAMES LEWIS

I didn't get a chance to read the article being here at the workshop. If you could describe to me make I can answer the question in terms of is this something

>>JAMES LEWIS

>>MALE SPEAKER

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 was going on on the computer by the actual person so that there were concurrent sessions going on--

>>JEFFREY FRIEDBERG

Any time 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 these things called automatic updating because we're constantly vigilant looking for these kinds of issues that come up and we create these if I can. 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 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 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 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 as pointed out earlier, don't reset passwords to other names, defaults aren't always set, what I call weekend settings. So it's still people's responsibility to some extent to make sure they have their defenses and 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 is because of this reliance on this sort of personally identifying information? Because that's what you can extract from people and databases.

>>JEFFREY FRIEDBERG

Let me try that 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 you can it will I'm going to say it's why we shouldn't be doing it. Having that up there but we 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 not making full use of it or we're making full use of it and gets to market fuel your point, we're going towards making full use of it as a slower pace than we would if we had these enabling measures like better identity manage. Better authentication, there's net stuff you can do with Internet technologies with-- in terms of buying, in terms of what Consumers could do. One example would be suppose you want to go out and negotiate. Sorry. I'll talk really close. 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's opportunities we're missing because of poor authentication. So one of those things we want to talk about is how do we defend ourselves against attacks? The other thing, how do we enable the next steps? I see Mike Nelson is raising his hand. You going to say net 2.0?

>>MALE SPEAKER

Mike Nelson, bip. I want to pick up on Jim's point and talk about the recurring theme of the last two days, interoperability. We tend to focus in these meetings what the consumer does, what happens at that time key board, what the smart card looks like. But there's half the problem we haven't talked much about, that is what happens in the back office systems and storage systems that's where a lot of compromises are actually happening. That's where the lost data tapes are ending up in the hands of hackers. There's a lot of neat to focus on that-- need to focus on that piece as well. -- focus on that piece as well. We need to get common standards, interoperable systems. I would like discussions to barriers about interoperability. We haven't talked about what standards can and need to do in this area. We have 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 decided it would only accept documents in word. -- documents in word. We have had government agencies that have said web authoring tools only work with certain web browsers because they're not standard products. Going forward governments have to be acutely aware of the standards their products support and they have to push industry together. Our natural tendency is to go in lots of different connects. 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's not good for the vendor to tell you it works together, we have the find ways to make sure these products are working together at the user end and back office. That's where the most exciting new opportunities are going to happen, as Jim said we have in the 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.

>> Interoperable trustworthy systems.

>>MALE SPEAKER

I would like to respond to that. One of the problems with the Internet, I think most people understand, some people anyway, 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 doing on the Internet. -- dog on the Internet. To fill the gap people came up with solutions over the years. There's things like X 509 certificate, token, ways to represent claims people make. The observations here is let's say you have to pick one of these, and bet on the right horse, make sure it's not the beta versus VHS situation. It's a huge challenge. Which to pick? So this is one of the catalyst for what's called this identity meta system, a system of systems because you don't want to have to ever pick the right one. There's an abstraction being done at a higher level. If you stick at the level, you can plug in all these systems today hence trying to drive this interoperability. That's why people are enamored by cart space and cards and things like that. When you have this system where you have somebody vouching for you who is an identity provider and you have a merchant, God knows what systems are actually running. They have to talk common languages. So I think this whole movement towards meta system is a really good one for us. I encourage everyone to spend time at the break-out session to hear more about it.

>>MALE SPEAKER

First off, I think you're absolutely right with the meta systems. I want to hit on the

interoperability. I'm with the Department of Defense access office. The interoperability is a huge deal we're working on that. You asked the question originally what government's role is. First off, to me it's very clear the 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 how far is putting together dynamic roles and laws. For example, one says it has to be compatible 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 does it take to get the real ID rule? You're not the only one in the room that actually likes that. But I think-- there are answers and I think we have heard all this-- one of the common themes is that's no one solution. Tough take all the solutions together and piece them where they're appropriate. Department of Defense has integrated or started using cryptologic log on. In one year we've seen a 50% decrease in successful attacks that's where does it solve the problem? No but it's a big part. 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 HSP-12 that nobody is looking at yet or there's two pieces, number one is the preissuance 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. 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, 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 make sure we still interoperate which is what you were talking about? That is huge, huge issue. 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 have a system out there and actually COD will probably be the last ones to implement HSPD-12 because we're the closest to start, sounds kind of counter intuitive 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 to 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 or trade it. I'm going to protect your information. You should come shop with me. I think that's going to be something getting people moving forward because we heard it has to be convenient and has to be something the consumer wants to grab

>>NAOMI LEFKOVITZ

Take AVIVA than Phil.

>>FEMALE SPEAKER

I think we personally maybe talking about the wrong issues. I think the role of government is to create skin in the game. So if you look 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, between businesses, the Internet is everywhere, in printers, gas pumps, we're never going to get a handle on it. I think the market will take care of solutions if government creates financial incentives and regulate it is right thing. 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, may have used paypal, other non-conventional money schemes where it's hard to recover. Also why doesn't government look at regulating all these information brokers out there? We can 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 consumer's back when they lose money. In my view that would be the right question for this group to address.

>> Okay.

>>MALE SPEAKER

Could I speak to that just for a moment? I think that there's 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, 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. Criminal organizations don't steal information for 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 that 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.

>>MALE SPEAKER

Phil (inaudible). To go back to the first question asked about government involvement and so on. Certainly information 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 wouldn't be operational for us. And the other thing here is that the U.S. has bought Ft. immediate. Other governments has their Ft. immediate. Just as everybody has people spying on everybody else, there are people spying on the U.S.. The other problem is terrorist are non-government tactics and they maybe more seriousch one thing that happens when whenever there's an international crisis now is you have hackers on both sides piling on. One of the big fears is maybe some of these hacker groups may cause a crisis to escalate when the diplomats are trying to deescalate. The other final point is must be. The thing that differentiates a terrorist from a terrorist organization is money. The bottom line half robbed banks in West Germany for many years. IRA protection raquets, kneecapping. Al-qaeda, essentially they have bin Laden's inher tense and once they 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 Mafia, almost all of them have their roots in some -- this is a nationalist security here and it's not being scare mongering to raise it.

>>NAOMI LEFKOVITZ

John and then I think there's some others that have been waiting.

>>MALE SPEAKER

Gregory I asked Steve crocker to try to attend

today because I have always argued with them that the initial design of the Internet while providing nice identification of the vices and do mains ignored people. And it's one of the critical challenges. We take for granted how individual the 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. For you personally, maybe for others on the table, can we talk about guaranteed secure email delivery? Seems to me one of the prototypical services we should be look for in the future that may help us flesh out not only organizational framework but the way to get there.

>>MALE SPEAKER

That's a huge project, John. Guaranteed secured e

>>GEORGE CRABB

We've had a lot of conversations in the postal service, I was 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 email of choice? And if you get what you want, you know, that's good. I think there's a lot of business need for guaranteed mail. Can-- if you receive

an email 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 email 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 is so dispersed that-- is it 90% of email communications today are Spam? That's a major problem. How do we get authenticated email, how do we do that infrastructure? There's 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 email.

>>NAOMI LEFKOVITZ

I'm going to pull us back one moment to some of the earlier themes and I wanted to pick up on something-- 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 identity 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 that-- 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. So these answers to that.

>>MALE SPEAKER

My name is Peri (inaudible) with (indiscernible). 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 P cash 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 tap or swipe on my credit card at a restaurant or using my card at TJX. That's a fundamental problem. 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 be an inconvenience to me. My bank or TJX, TJX maybe a

bad example because they are pay 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 organizes. 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 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 how to get those back in alignment? I'm going to take Gail and then Fred.

>>FEMALE SPEAKER

I think it's going to be extremely hard for the market acting by itself to set the bar in the right place for very rational reasons. Businesses spreading that loss over all customers. It's a small amount per customer. For individual who is in that X percent, maybe it's 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 that loss allocation and internalizing that risk is going to help change the technology investment equation but I think even as you look at risk-based authentication you have to be 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, just going to talk about evaluating X risk and not Y risk, you need to pick up on both of them. In the confinement space Consumers have expectations that will not be met. I talk to financial writers all the time who think you have charge become on your debit cards. We know the statute doesn't give you that. As we

move in immobile payments there will be devices that can be tied to credit cards with excellent consumer protections, a debit card, and to a prepaid account if it's not linked in some way to a deposit account you have no REG-E and there's a role for FTC to set those goals on the front end before the mechanisms become widespread.

>>FEMALE SPEAKER

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

>>MALE SPEAKER

Fred Schneider Cornell. I want to amplify those comments and put it in a slightly different way. Your opening remarks were about the market and whether the market is working. And it's clear it's not. It's not working for two reasons. One, 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-technology technologists to know about it is maybe a good way to spend a day and a half. I think you missed the point completely. 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's happened, I won't be surprised if various industry groups go to stronger authentication mechanisms. The credit card company also have a great incentive to have authentication instead of identifiers of the authentication. But that's more natural than imposing a solution. I think there's an inflection point and you're not looking at it, and AVIVA was pointing to it and the attorney from consumer union is pointing at it,

that's the real opportunity for government to have leverage. It's not by thinking about technological solutions which will move faster than the government can move even in the absence of attackers which seems to move at the same speed as technology.

>>MALE SPEAKER

Can I make a point to follow-up? I think that's right basically. Governments create the conditions for markets to work, for markets to work better. In this particular case the cases that we're talking about, it has to be minimal light weight regulatory approach. Has to be technology neutral. All the stuff we say. But we have to address two fundamental issues that the government would only address. And the first is liability as we have here, the second is trust. How do we create trust, how do we link the individual and the identity to the machine or software? Those are the two places-- 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?

>>MALE SPEAKER

I can tell you one of the things that Fred brought up which is critical which hasn't been talked about I think enough in the conference is this issue of the privacy concern. That as we go forward looking for a stronger way to authenticate and things of that nature will'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. Someone mentioned earlier how the latest REV of some bill didn't have the word privacy in it at all. It was removed. So what does that tell you? 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 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-- do we mean comprehensive, sort of comprehensive and comprehensible, because isn't that part of the problem that we're talking about that Consumers don't understand intricacies of HIPAA, they don't understand the FCRA, they don't understand where the holes are so they can protect themselves. Do we need something comprehensible?

>>MALE SPEAKER

Yeah is the short answer with the caveat learn from the European experience which is 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--

>>MALE SPEAKER

(indiscernible) sun micro systems. I would like to come back to the issue of liability. I think liability might be one of the great drivers and 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 I believe a couple of minutes ago you mentioned that for instance in the difference between BJ's security breach at BJ 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 experienced 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 federated approach. Where not necessarily every shop, every participant in the market, every part of company sets up their own identity information but starts to trust certain

other companies that specialize in providing identity. That 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 tha

>>NAOMI LEFKOVITZ

Tom.

>>MALE SPEAKER

Just first a quick comment on privacy and identity. I think different identity regimes have different implications for privacy. There's a discussion by Gregory and Jeffrey about shared secrets. And one of the issues with shared secrets in an environment where you-- information is available is that secret you have to choose becomes more and more personal in order to defeat the fraud stir. There's an interesting study I recommend for folks to look at by Alexander QUICY from Cornell, look at the amount of information disclosed in their face book accounts. A typical consumer might disclose information like favorite books, the school they went to, birthday, SSN. Amazing what people will disclose. Tough think about that so if you're relying on shared secrets there's a privacy implication. The other point to make related to a role government I think would have is promoting research in this area. One thing I have had experience working in this field a number of years is the divergence of statistics and assessing 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 at my own company has done we have not seen any indication of that rate. That's one example I think we need to do more research.

>>MALE SPEAKER

>>FEMALE SPEAKER

(inaudible). I want to shift focus here, 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 of an extent of the problem itself. In that regard I would 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 AT&T 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 as a condition of underwriting their fraud losses disclosing the fraud incident data to begin with and then we can start to get a 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 of the solutions these authentication solutions we're proposing here.

>>JEFFREY FRIEDBERG

One other theme I didn't share with you is check the math. This has to do with scrubbing the numbers. Since a lot of public policy is based on what the perceived statistics are, it's critical that we have reasonable metrics that we understand what we're looking at. Different ciebdz of fraud, how it's happening. There's a know men clayture problem all over the place. And a lot of people were 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 AI of us. I should be international also so that we actually can see that the trends-- so great idea.

>>MALE SPEAKER

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. We-- if we were a corporation we would be 21st in the Fortune 500. Our revenues are about 73 billion a year. How does an organization that size that has a public mandate that services everyone in the United States maintain trust? Well, first of all, accept for a change of address system where we keep the records for one year, we don't associate any identity to the address 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 I put up on the screen, they're hiding within the percentages. And's not 2%. Identity frauds are not 2% of most organizations. It's typically .1 of a percent of fraud for a particular organization. But that .1% represents billions of dollars of fraud that need 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. That's-- and a lot of criminality can be committed by the billions of dollars that little percentage represents.

>>NAOMI LEFKOVITZ

Yes.

>>FEMALE SPEAKER

>>MALE SPEAKER

Martin boz worth, my publish info. I know we're short of time so I'll read you. This just came in while here at the conference. Computer equipment containing the perm data of nearly 160,000 current and former employees of the Neiman Marcus group has been stolen. The equipment has been own bid a third party consultant not named. The the stolen files contain data from 2005 including Social Security numbers and salary information. This just happened while we were here. There are so many things that go wrong in that statement I don't know even where to start. First, the fact

they outsourced this information to a third party when you open up your data chain, the more you open it up to the more weakness you'll have. The human factor is the biggest weakness. Would we have even known about this if there was not mandated information? Of course not. Anybody that could afford to shop, 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 not theirs to begin with. We talked about this conference about authentication technologies, multi-factor authentication. All this stuff is extremely important and necessary but none of that played in this scenario. It was somebody who misplaces a computer or left it in a car or their house and it got stolen and they don't even-- 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 slot. You can't say the market will 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 to address them. I'm sorry for the speech

>>MALE SPEAKER

We did discuss the pregnant the leak strategy which is critical which addresses some of the insider issues that can happen, the lost laptop, things of that nature. That's an awareness by some companies that they need this data stray data strategy. I mentioned the auditing and reporting capability which is when things get abridged 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 it's not a free lunch, not that easy to do. It's steps in the right direction

>>MALE SPEAKER

Really quickly let me 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 heard it's terrible for individuals, 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 compa

>>NAOMI LEFKOVITZ

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

>>FEMALE SPEAKER  
Looks like an inside job. You would think at the end of this conference it certainly is a tearful thing all 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 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 get a point in our discussion where that doesn't matter because we achieved a better form of authentication and disincentivize the data thieves so they're not looking for the data any more because we have stronger ways to ensure once it's stolen it can't be used.

>>NAOMI LEFKOVITZ

We didn't set this up but perfect segway because we have a few minutes left and I want to talk about the action items that I have on my list. For government I have fixed the imbalance in the market.

[laughter]

>>NAOMI LEFKOVITZ

And after that we're going to fix the liability problem. And we're going to create trust. Maybe we can posit that perhaps we need a more 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 ta

>>MALE SPEAKER

Interoperability.

>>NAOMI LEFKOVITZ

So you guys can work on that. All right.

[laughter]

>>NAOMI LEFKOVITZ

And finally--

>>MALE SPEAKER

Think ease of use was in there too.

>>NAOMI LEFKOVITZ

Ease of use. Great.

>>FEMALE SPEAKER

Liability.

>>NAOMI LEFKOVITZ

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

>>MALE SPEAKER

Consumer versus no choice (off mic) sitting ducks (off mic).

>>FEMALE SPEAKER

(off mic)

>>MALE SPEAKER

We need more information. (off mic)

>>NAOMI LEFKOVITZ

Okay.

>>MALE SPEAKER

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

>>NAOMI LEFKOVITZ

A responsibility.

>>MALE SPEAKER

The first \$50 is yours. (off mic) liability on the individual. I can lose my wallet. It isn't just a computer. But it's got to be--

>>MALE SPEAKER

At the end of the day if I had asymmetric keys, 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

>>MALE SPEAKER

(off mic)

>>NAOMI LEFKOVITZ

All right. Demand security.

>>MALE SPEAKER

(off mic)

>>NAOMI LEFKOVITZ

Thank you very much. This is going to conclude this panel. We are now going to have closing remarks from Lydia PARNEZ Director of bureau of consumer protection.

>>FEMALE SPEAKER

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 a distinguished set of Pamists and moderators about how we can improve our modification systems to help reduce identity theft. It's so obvious just listening to you these 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 identity 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 more buy-in from all of the stakeholders. The opening panel, Simon Davies and Gus HOZAN talked about the necessity of five Ds, discourse, deliberation, 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 life these considerations, it-- in light of these considerings 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 benefits 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 of authentication technology was 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 from a broad range of technologists that can help us-- 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 greater convenience in their daily lives. Ways 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 a 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 the foundation for a healthy market by ensuring consumer trust and supporting an infrastructure from 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 cooperatening 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, Joannena, Kristin, Stacy and Alicia. Can you all stand up?

[applause]

>>FEMALE SPEAKER

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 break-out sessions. Thank [applause]

[Captions performed by Caption IT, LLC,  
[www.captionit.net](http://www.captionit.net)]

>>NAOMI LEFKOVITZ

Let me tell you about the logistics before you disperse. If you're come back for the break out sessions this room is going to be divided type three rooms so you look on your agenda, you'll see the room number or letter actually. And you'll see the room letters outside the doors. Okay?

[Captions performed by Caption IT, LLC,  
[www.captionit.net](http://www.captionit.net)]