TRANSCRIPT

PROOF POSITIVE:

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

>>JAMES LEWIS

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

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

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

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

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

We have a lot of things going on in the authentication space. And there are some things we can draw from that. The first is, and this came up a little bit in the last panel, one size does not fit all. People will not want a really strong, roborth2ces ot of thin -1.1who7I0.0 does not fi

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

>>NAOMI LEFKOVITZ

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

>>GREG CRABB

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

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

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

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

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

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

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

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

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

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

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

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

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

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

And this is going to be a very controversial point that I'm going to make. A couple of weeks ago I was in the UK. A serithe consumer. And t gtecern4 Tw 3 -1.13hsxpanwa

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

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

And for myself, I really didn't have any choice but to create some kind of picture just so I could externalize and sleep at night. That ended up becoming this thing called the Internet battlefield which I have shared with a number of people in the room. I'm just going to show you a picture of it now so you can look at it. It's a little scary and it looks really complex. I normally take about an

This leads us to the next theme which is, really, don’t share s

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

>>JEFFREY FRIEDBERG

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

>>AUDIENCE MEMBER

Well, it might be a good idea to look at it, but I think in general it was an exploit where people from another country were getting into the utility software that's used generally on most people's computers like Microsoft Office and things of that nature. And getting into the machine to the extent wh

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

>>NAOMI LEFKOVITZ

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

>>JAMES LEWIS

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

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

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

>>AUDIENCE MEMBER

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

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

area. We have got lots of examples wh

>>AUDIENCE MEMBER

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

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

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

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

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

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

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

>>NAOMI LEFKOVITZ

Take Avivah then Phil and then come back.

>>AUDIENCE MEMBER

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

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

>>NAOMI LEFKOVITZ

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

>>AUDIENCE MEMBER

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

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

>>GREG CRABB

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

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

>>NAOMI LEFKOVITZ

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

>>AUDIENCE MEMBER

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

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

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

>>NAOMI LEFKOVITZ

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

>>AUDIENCE MEMBER

I think it's going to be extremely hard for the -- Gail Hillebrand, Consumer's Union -- for the market acting by itself to set the bar in the right place for a very rational reason: businesses spread that loss over all of its customers. It's a small amount per customer. For the individual who is in that X percent, maybe it's the 2%, they're suffering that loss themselves, at least the inconvenience loss, the stress loss, the family emotional incidence. Maybe they'll get their money back, depending on how the money was stolen and where stolen from. I agree with Avivah that loss allocation and internalizing those risks by putting them on the business is going to help change the technology investment equation, but I think even as you look at risk-b

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

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

>>JAMES LEWIS

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

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

>>NAOMI LEFKOVITZ

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

>>JEFFREY FRIEDBERG

I can tell you right now that one of the things that Fred brought up, which is really critical, which hasn't really been talked ahe thiwe create trust 2001 Tc -0.0t solutie Tc -0.0prt acy(r .66r an)T

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

>>JAMES LEWIS

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

>>NAOMI LEFKOVITZ

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

>>AUDIENCE MEMBER

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

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

One way of doing that might be through -- to go through a federated approach. Where not necessarily every shop, every participant in the market, every part of a company sets up their own identity information, but instead starts to trust certain other companies that specialize in actually providing identity. That kind of trust would grow naturally out of the market wi.15Lfn(naturally ze 6p/90.00c07 Tw -1h2BDC identity. 311 T05 0 Td(of tr)Tj

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

>>NAOMI LEFKOVITZ

Tom?

>>AUDIENCE MEMBER

Just first a quick comment on privacy and identity. I think different identity regimes have different implications for privacy. There was a di

privacy preserving way. There's a layer of abstraction that this information can be shared and we can get a better understand

Yes. Am I missing anybody over here?

>>JAMES LEWIS

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

>>NAOMI LEFKOVITZ

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

>>BETSY BRODER

Looks like an inside job, right? You

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

>>NAOMI LEFKOVITZ

And finally –

>>JEFFREY FRIEDBERG

I think ease of use was in there too.

>>NAOMI LEFKOVITZ

Ease of use. Great.

>>AUDIENCE MEMBER

Liability.

>>NAOMI LEFKOVITZ

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

>>AUDIENCE MEMBER

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

>>NAOMI LEFKOVITZ

Okay.

>>JEFFREY FRIEDBERG

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

>>NAOMI LEFKOVITZ

Responsibility.

>>AUDIENCE MEMBER

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

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

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

So yesterday afternoon we heard about a broad range of technologies that can help us better authenticate individuals. One theme that emerged loud and clear was that no one technology will be a silver bullet. To

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