PANEL 2: CONSUMER TOOLS FOR MANAGING INFORMATION SECURITY

MR. SILVER: Welcome back, everyone. This is panel two, which will focus on the tools that consumers currently have to manage their information security.

We will look at tools that exist both online, and also some tools you may have currently in your pockets right now. We will also examine how consumers can best use these tools.

I will begin by introducing our panelists, starting at stage right over there. Anson Lee is with Symantec Corporation, Mark MacCarthy is with Visa U.S.A., Rich Lloyd is with Dell Inc.

Alan Paller is here from the SANS Institute. My colleague, Loretta Garrison, will be helping me today, from the FTC. Michael Willett is a security and privacy consultant, Larry Clinton is with the Internet Security Alliance.

And Richard Smith is an Internet consultant. He will be leading us off with an overview of the kinds of tools that are currently available online to consumers.

MR. SMITH: Okay. What I want to try to do is give the 10,000 feet view of security products that are available that we use everyday, or many of us use

everyday on our home computers.

In the first session, there was a lot of talk about the use of SSL, or HTTP secure socket layer. It's an example of a technology, I think, which is the most appropriate, in that it just works. It's not something that a user necessarily has to turn on, or specially use in order to get security.

The primary purpose of SSL is to encrypt information that goes between a home computer and a website. So, if you're entering an e-commerce website, and you're buying something, you're providing your name, your address, your credit card numbers and so on, that information is scrambled on transmission.

And the main purpose of SSL is really to prevent eavesdropping, so that if you have got somebody that could intercept, web traffic, they can't look at the stuff. It all looks like gibberish.

And a good example of how easy something could be intercepted is if you're at work and you're buying something at Amazon, your network administrator has -- or other employees could very easily eavesdrop, because you have a shared connection at work.

But there are also problems with eavesdropping on wireless connections and these sorts of things. SSL has been a very successful technology, and overall, has

worked very well. It's an example, I think, of one the best technologies. It's just there, it comes with the product, it comes as part of almost all web browsers, or at least all the ones that, 99 percent of the people of the world use, and it's been a great technology.

Another example of a technology that's built-in, that I like for security, is in Outlook. If we think of a virus problem here, which I will get into next, many of us are very familiar with anti-virus software. It's a kind of software that we buy in order to provide protection.

There is also anti-virus protection, though, in Outlook now. A lot of the viruses that we get, and worms that we get, come through as e-mail attachments. And Outlook, for the last couple of years, will now automatically delete any kind of executable file that comes in as an attachment.

And I find that is a very effective measure. I don't have to worry about keeping an anti-virus software up to date. And it's very transparent. The only problem is if someone -- if a programmer friend sends me an executable and forgets to zip it up, then I have to send him back an e-mail, "try again." But that's just teaching good computing practices, basically.

Another form of protection from viruses, of

course, is anti-virus software. It's probably the most famous kind of security protection out there. The whole idea is that you run a software program in the background on your computer, and as you access files, before you run them, it checks -- or at various times checks -- to see if these are known viruses or worms or Trojan horse programs.

What's good about anti-virus software is that it's, again, an automatic activity that goes on, not something the user has to do, but they do have to install it.

Now, the issue, the problem with anti-virus software is it can't really read the mind of the program, it can't predict if this particular piece of software has malicious intent.

So, with anti-virus software, it's said the way that it works is it has a database of known viruses or worms, and there are thousands or tens of thousands of these programs in the database. And there are little signatures that say, okay, for this particular virus, we know this pattern appears in the program, so if we ever see that in a file, it's most likely an infected file, or an example of a worm. And therefore, we can warn the user of it.

It's kind of insurance policy-type software.

Not everybody gets infected with a virus sent to them. So a lot of things with security, we do have to keep in mind is that they are like insurance. We don't always do it.

Everybody who owns a house has fire insurance, but we don't expect a fire in the house. And a lot of the security aspects that we get into are the same way, that we may, in some sense, not need this software, but we have to have it anyway, just in case.

In terms of new viruses, there are tens of thousands of people out there in the world writing viruses around the world, literally, and so we have, every month, 10,000 new viruses, maybe -- I don't know what the numbers are, maybe Mr. Lee from Symantec could give us a number -- but we need to keep the anti-virus software up to date. And now it's basically on a daily basis.

With the Internet, new viruses are being released and spread within days. So, that's one side of it. The anti-virus question is how we get updates. And through the Internet, it's pretty easy.

How do we get viruses on home PCs? That's just one thing. When we talk about security measures, we want to talk about the threats. And just really briefly here, we get them through e-mail attachments as a primary

method.

And as I mentioned, Outlook will now automatically block certain things so it can provide -- software itself can provide anti-virus protection. We download files from websites. There are security holes that are in web browsers that allow automatic execution of viruses or worms or Trojan horses, inside Word documents -- although that's becoming less prevalent because of some changes that Microsoft has made.

People just love whatever technology is popular through P2P networks -- not to be confused with P3P -- but through song-sharing networks, like Kazaa and Morpheus, and then instant messaging is another way it's becoming popular. Basically, any time you have a network connection and get data this way you're going to get a virus.

Another security technology for home PCs are firewalls. Firewalls began their lives more in the corporate or university settings. We had this concept of a local area network with a whole bunch of computers on it, and you had the evil Internet out here, with all the bad guys trying to break in. And so a firewall is basically a moat, if you will, around -- or a wall around -- that internal network.

So we have trusted computers inside, and you

have untrusted computers on the outside. And a firewall then blocks traffic coming in from that untrusted world into your local area network.

For a home PC, the definition of the firewall has grown, but you can have the same issues. At my household, we have three computer networks. We have one computer for each person, so we have a little local area network. And so we have some trusted computers, and then we have the outside, untrusted world.

And we use what's known as a router box in order to provide the firewall protection. It protects us from any kind of hostile intent that's coming in. And that can be basically hackers trying to break into computers. And the way that they do that is they look for services that are running on unprotected computers, and try to exploit security holes that are in there.

Another thing, though, that the home firewall does is it also looks for what is known as spyware, that is, programs that get loaded on your computer that want to phone out with personal information, or more typically, your web browsing history. And you will get spyware installed on computers through, basically, downloading software, say, like on a Kazaa or Morpheus.

My daughter -- I keep telling her to stop doing this, but she keeps installing Kazaa on her mom's

computer, and so I have to keep cleaning it off the various packages.

What's interesting is anti-virus software, in general, does not look for spyware. So the moral of the solution is see that when a spyware program tries to phone home, the firewall alerts you that somebody is trying to go out. Here you have the trusted computer trying to go out to the untrusted Internet.

And in general, the rule of thumb is that if you're running on a cable modem or DSL connection, a firewall is more important to get, because your computer is going to be online more, and more vulnerable to outsiders trying to break in.

The last kind of software I want to talk about is a spyware detector. As I mentioned, many of the anti-virus software packages today don't look for spyware, and there are many different flavors of it. But there are new packages that are coming out from other companies that work just like anti-virus software that look for signatures, but they look specifically for spyware.

And I have three categories here. One is keyboard sniffers, commercial spyware, and Trojan horses. A keyboard sniffer is a program that simply records all the key strokes that happen on a keyboard, and sends that information off to someone else. There are probably a

couple of dozen packages you can go out and buy, or even download for free, that do this. They are typically sold for one spouse to spy on the other spouse. That's the main market for this software. They are also used sometimes for spying on employees, and so on. But where they really become dangerous is if an outsider uses it to, say, steal credit card numbers, and so on.

And this is how you get around SSL, by the way. If you want to be an eavesdropper, you spy on somebody before data gets encrypted.

So, commercial spyware are packages that provide, for example, pop-up advertising, based on what you're searching for at search engines, that sort of thing, and then you have Trojan horses, which anti-virus software do generally look for.

I will just give you quickly one war story here to sort of wrap it up, of the dangers of keyboard sniffers, which is one-fourth of spyware. A gentleman named Douglas Boudreau at Boston College installed 100 keyboard sniffers around the campus of Boston College, and he was caught.

And he collected personal information on more than 5,000 people in the Boston College community, faculty and students. And he got everything all these people typed on the keyboard all day long. He was just

constantly collecting this information which was being sent off to a server he was running.

And he got account names, password, credit card numbers, PIN numbers, you name it. You know, if you're doing online banking you have to provide your PIN number. So he got it all. You can just imagine -- personal e-mails, just the whole gamut.

A lot of computer crooks, though, don't actually make good criminals. He didn't monetize, if you will, all this information being collected. And he only ended up stealing $2,000. And therefore, when the State of Massachusetts went after him, the state decided not to throw him in the pokey for 20 years, but just put him on probation for a few years. I thought that was a little bit light for the sentence.

But it just shows you some of the dangers here of these kinds of software that are out there, some of the threats that are out there. And when we get smarter criminals out there who are using keyboard sniffers, they could steal, actually, a lot of money. Thank you very much.

(Applause.)

MR. SILVER: Thank you, Richard. Now that we know more about what tools are out there, it's important to know both how and why to use them.

Larry Clinton is with the Internet Security Alliance, and he's going to speak a bit about why tools are needed, and what home and individual users should do.

MR. CLINTON: It's not a little television set. If there was one thing that I think I want consumers to understand about their home computer is that it's not a little TV. It's not a dumb, inanimate object that you sit down in front of and just drink stuff in.

Your home computer, particularly when connected to the Internet, is like your friend, your really, really, smart friend. Or maybe, better yet, your home computer connected to the Internet is like your very gifted child. You need to develop a relationship with it, you need to work with it, you need to communicate with it, you need to take care of it. And if you take care of it, it will take care of you. And you will learn wondrous things.

If you don't take care of it, you could have trouble -- a lot of it unanticipated -- and a lot of it very, very tough to deal with at later stages. So, what we are focused on for the moment here is not so much the technology as much as the behaviors that consumers need to adapt in order to become better computer citizens.

I'm going to deal with the first two parts of my presentation fairly quickly, who we are and why we

must take action, so I can spend, hopefully, more time on what it is we should do.

The Internet Security Alliance is a collaboration between the Electronic Industries Alliance, which is a 1,200 corporate member trade association, essentially, located over in Arlington, Virginia, and the CERT Coordination Center, at Carnegie Mellon University, which is pretty much the granddaddy of all the CERTs, and one of the experts, one of the leading experts, in vulnerability and threat analysis.

These are our corporate sponsors, these are the members of the board of directors. I point this out primarily to distance ourselves a little bit from most of what we're discussing today. The Internet Security Alliance is primarily focused not on individual consumers, we're really focused more on the corporate security level.

Last summer, we came out with this publication, "The Common Sense Guide for CEOs and Senior Managers for Internet Security." It's been pretty well reviewed. It was cited in the national strategy -- draft strategy -- TechNet has endorsed it, the U.S. council is now endorsing it, some overseas people are doing it.

After we came out with this, a number of people said, "Well, look. This is great. Why don't you come

out with something for the individual user?" And so we have, although frankly, it's not our main focus.

I think the primary benefit that I can offer today is not so much the content of what I'm about to say, but to simply provide consumers with a place to go where we have organized this information. So, we have one of these guides specifically for consumers and end users located on our website, isalliance.org.

Why we need to act? I think most of us in this room are pretty well familiar with this. This is a picture of the Internet as it was originally conceived, or thought of back in 1980. And at the time, this was thought to be very, very complex. This is the Internet now, graphically illustrated.

And by the way, it's kind of interesting. If you look at this, you notice that really intense kind of purplish area right there? I'm pretty sure that's the FTC.

(Laughter.)

MR. CLINTON: Here are some of the threats and attackers. Again, we have already gone over a number of these. The human agents are one of the things we're most concentrated about -- hackers, disgruntled employees, white collar criminals.

And I agree with the previous speaker, they're

going to get smarter, they're going to be involved with organized crime. Terrorists have received a lot of attention, and perhaps the fact that they may couple a physical attack with a subsequent cyber attack, which could be very threatening.

All of us on 9-11, I'm going to bet, did pretty much the same thing, which is we reached for an information system. We grabbed the telephone, we turned on the TV, we got on the Internet, and we were able to be reassured by the fact that we were able to see what was going on.

Imagine if the information systems were attacked and they went down, and we didn't know if there was a simultaneous attack going on in Florida or California, or if there was a chemical attack coupled with a physical attack. So that's very important on the terrorist level.

The one thing that we don't have on this that a number of people pointed out to me is we probably need to add another bullet, which is for pimply teenage kids in their basement. Very threatening human agent. Twenty-five of all the Internet attacks happen on Saturday night. One of the solutions we are looking into at the Internet Security Alliance is developing a website, GetaNerdaDate.com.

(Laughter.)

MR. CLINTON: We figure if we can get a lot of these kids out of their basement on Saturday night, we can do an awful lot to help with the Internet situation.

This is just the number of incidents reported to the CERT/CC. The actual numbers are not particularly interesting. What's interesting is the trend line, and actually, these numbers are vastly, vastly under-reported. Internet attacks are going way up, and here is the reason why.

As the sophistication of attacks is increasing, the amount of knowledge to create an attack is decreasing. So it's becoming easier and easier for all of us to use the Internet, it's becoming easier and easier for people to break into the Internet and cause us problems.

So, we finally get to what we should do. And this is the items that we have listed in the individual user common sense guide. I will go through them fairly briefly. A number of them have already been touched on.

The first is to use an anti-virus program. If there is only one thing that a consumer can do, for financial reasons, or whatever, this is what we would recommend, number one. We think it's your single best defense. Obviously, there are many ways to infect your

program -- floppies, CDs, e-mail, et cetera. Some of these programs will check these things automatically. Sometimes you have to check to see -- or sometimes they will check simply for the signatures.

There are new devices, that contain heuristics that actually go beyond the known signatures. The problem with these is that they tend to slow down service. And this is the real test that we have to get past, is what is the trade-off between increased security and increased functionality?

One of our big problems, on the behavioral level, is people turn off their security devices. One of the reasons why the vendors don't want to put out really secure software is consumers don't want it. So how do we deal with that problem? It's a major problem.

Number two is to keep your system patched. When the system acts erratically, obviously you want to know why. Usually you can contact your vendor. Some vendors will notify you automatically if you ask them to. Again, one of the problems is sometimes the patches cause additional problems, and sometimes even the vendors aren't aware of these problems.

So again, we need to have an interactive system, we need to work with the vendors, you need to tell them what's going wrong with your computer.

Number three is to use care when reading e-mails and attachments. I think by this time we're all pretty familiar with getting physical junk mail, and there is no real problem with reading any of that. But we all know that you have to be very careful with what you respond to when you get things electronically. Obviously, you don't even open it unless you know what's going on.

And the single best test for this -- and this is why we call it the common sense guide -- is does the message make sense. I remember, and I think it was back in 1998, when the I Love You Virus came through, I was fortunate, because the first I Love You notice I got came from somebody I did know, and I knew for a fact she didn't love me.

(Laughter.)

MR. CLINTON: Make sure the stuff makes sense. Number four, install and use a firewall program -- I think this has already been talked about -- a firewall is kind of like your security guard. It tells the packets where they can go and what they can go.

Now, the real hard part of the firewall is that eventually, you, the consumer, have to figure out what are the rules for what information should go here and there. Again, you must learn your computer, you must

know your computer, you need to work with your computer in order to make it functional and secure.

Number five, make back-ups of important file folders. A lot of us have fireproof boxes in our houses where we install our wills or vital information, maybe some pictures of our kids, or whatever. You need to do the same thing.

I know most of us -- I know I did -- learned the message the hard way with my first computer. I was in my first office, I lost my file, and the system manager came to me and said, "Did you save it?" And I said, "No, I wasn't finished yet." You save as you're going along. How often do you have to do this? Pretty often, unfortunately.

Number six, use strong personal passwords. One of the things that, behaviorally, we find we still have major problems with, everybody has got a password, and a lot of people have them right where they can see them on their cubicle, so they remember their password, and anybody can come along and get it directly.

Good passwords are strong, which usually means longer. They are unique, so you don't use "welcome" for all the passwords. They have to be remembered. You shouldn't be writing them down. And they have to be changed fairly often.

Number seven, you use care when downloading and installing programs. A lot of us get CDs in the mail. "You don't know where that CD has been," you tell your smart little gifted child computer, so you don't put it on there unless you are familiar with it. You have to consider the cost benefits.

Number eight, install a hardware firewall that's very similar to what we have already discussed.

And number nine, use access controls and/or encryption. A lot of us who have had kids know that early on, you spell things so that the kids don't know what you're talking about. That's encryption. And later on, the kids learn how to spell, so you have to use other sorts of things. Pretty much the same thing with your computer.

Again, it's not a TV, it's like an organism. You have to deal with it, you have to grow with it. If you do, you can make it secure and functional.

MR. SILVER: Thanks, Larry.

(Applause.)

MR. SILVER: Before we go on I just want to say we're running a bit behind schedule, so I would ask other panelists to keep that in mind.

Well, we know what the tools are, we have identified some of the threats that are faced, and we

have learned how to use the tools against the threats. So, a remaining question is whether consumers are actually putting these tools to work.

And I wanted to direct this question first to Anson Lee, of Symantec.

MR. LEE: In regards to the tools, yes, they are readily available. And we have talked about them: AV, anti-virus, firewalls, spyware detector, and the like. But unfortunately, most users aren't aware of these tools, because they aren't aware of the dangers that there currently are when they go on the Internet.

Most users don't really care about how the Internet works, or even how their computer works. They just want to know that they can get on the Internet when they turn on their computer and they log into their accounts.

What we have to do is to make them aware of these dangers, of viruses, of privacy threats, of hackers, and the like, that these things are constantly out there where we have individuals with programs and with these automated tools trying to find open systems to get into.

It's not exactly that they're out there looking specifically for Anson Lee's computer to break into, they're just looking for the first vulnerable target that

they can get into. And then when they're in, they can use those resources, whether it be the computer's hard drive, their high speed Internet access, or maybe whatever private or personal information is on that computer.

MR. SILVER: What usually leads consumers to purchase tools?

MR. LEE: Well, for anti-virus, it has usually been that they got infected, and they lost some data, and now they have to recreate that data. And now they have that experience of having been infected. They go out and purchase an AV product.

With firewalls and the like, it's usually because they are now hearing about Internet security threats, that they are adopting high-speed Internet access, and their ISP is probably telling them, "Oh, by the way, your computer is now on 24 hours a day, 7 days a week. If you leave your computer on, and your Internet connection is on all the time, you should think about a firewall."

But then users are thinking, "Gosh, that's a lot of work." A firewall typically is not an install-it-and-forget-about-it kind of program, whereas anti-virus is. You install it and you can forget about it. A firewall takes a bit of training for it to understand

what you're trying to do, what programs you want to allow to access the Internet, what types of activities you do on the Internet.

So it takes a fair amount of training. And for users, that's kind of inconvenient to them. They don't want to go ahead and train this program to be able to recognize, okay, this application or this program can access the Internet, while this other program cannot access the Internet. But again, it's all a matter of making users aware of the dangers of potentially what could happen.

And users also have this feeling of "Gosh, I'm just a home user, who is going to come into my computer? What's on my computer that's of value to anyone?" But for most of us here, we probably -- if we look in our computer, we've got a copy of our resume, more than likely we're doing our online banking, we're doing our online shopping, and what not.

These are all very important types of information, that if someone were to be able to get their hands on, it's prime to leading to identity theft.

MR. SILVER: Thanks. Software vendors are one source of information security tools, but PC vendors can also play a role in this area. Rich Lloyd is here from Dell to discuss some of their initiatives in this area.

MR. LLOYD: Yes, it's been a great panel so far. And certainly at Dell, we're excited about what we feel can be a pretty important role, as a PC vendor directly to the customer.

Before I get into what we're doing, I would be remiss if I didn't thank Larry for the new marketing concept. The PC as a gifted child. I think that will do very well.

In terms of what a hardware vendor can do, I think for a long time we saw ourselves as more of a facilitator. So we would be an early adopter of P3P. We would be a company that made Symantec and McAfee software readily available, provide custom-installed trial versions of the software, with the hope to snag customers and drive up the adoption rates.

I think we felt a responsibility to make as many of those commercially available tools available as possible. And for the most part, we sort of patted ourselves on the back as we were doing about as much as we could there. And then, of course, the data came back. And four percent of our customers told us they actually changed their P3P settings. Four percent. And about eight percent of customers actually took the McAfee 90-day trial and turned it into a purchased subscription.

We started thinking, is there a more proactive

role we can play? Because I believe the panel this morning was absolutely spot on. It has to be easy, it has to be transparent, and it has to be relatively costless. Because I would submit to you that the cost benefit analysis for an individual consumer around privacy is really somewhere in the $20 to $30 range, honestly.

And so, as a corporation, I have a fiduciary responsible to not break my commitments to Wall Street, and yet provide that kind of a value proposition. That's very difficult to do.

So, what are we doing? We believe we have got to change the paradigm a little bit at Dell. And we have got to make security and privacy really transparent on the box, itself. So, one of the things you will see us announce here in the next few days is factory-ready, installed Center for Internet Security benchmark configurations on the PCs, themselves.

And what does that mean? That means there is a level one benchmark, which Alan Paller will talk more about, factory installed on the system, that provides a little bit higher level of security and privacy on the machine without breaking things, that provides benchmark configurations for your OS settings that close off ports and do some other things that add just a little bit more

security than our traditional custom factory installs.

What we plan to do at Dell is to provide commercial offerings for folks that want to move up the grade, the security grade, and also move that out into other parts of our product set. I really believe that while demand for this kind of a product doesn't seem to be really strong in the consumer space right now, if we can make it transparent, if we can do it in a way that covers our fixed cost, and we can offer it on a variable cost basis, almost free or free, I really believe that you will see the demand -- which, right now, is fairly isolated to the public space -- move down into the consumer space.

And we're very, very excited about this thing. We have got to, as technology companies that have direct relationships with customers like we do at Dell, own up to the responsibility of making technology transparent. Because, unfortunately, despite all the good efforts of the W3C, of other groups that have done a really good job, in my opinion, putting publicly available technology in place, customers are not willing to invest, as was said earlier, the time, the money, and the effort to go about it.

So you have got to put it on the products they buy, and you have got to figure out a way to do it in a

way that makes economic sense for the market. And really, that's kind of the philosophy we're driving at Dell.

MR. SILVER: Thanks, Rich. Many of us shop online, and we may worry about our credit cards from time to time. Some companies are responding with tools to reduce the danger of using your card while shopping online. Mike MacCarthy, from Visa, will describe Visa's work in this area.

MR. MACCARTHY: Thanks, Jim. I want to talk about the Verified by Visa program, which many of you might have seen commercials about on television, but I want to give you some background about why we're doing it, what it is, and how it's working.

The Internet is the growing source of commerce for a lot of people, it's very important for our company. It's gone mainstream. More than 70 percent of all Americans are online these days. For Visa, it constitutes about six percent of all our retail sales. That's up from four percent last year, in 2001, and up from two percent in the year 2000. So this is a growing source of volume for Visa.

The channel is important to us for competitive reasons. We have 12 percent of all personal consumption expenditures generally, but we have well over 50 percent

of the retail sales on the Internet. So, electronic commerce is important for us to promote.

What is one of the major concerns that people have about shopping online? Survey after survey shows its concerns about security. "Surveying the Digital Future," a UCLA Internet report in February of this year, showed that 92 percent of all consumers are concerned about online security, 63 percent of them are very concerned.

According to research by a company called Payment One, released just last week, when consumers who have not made online purchases were asked what would persuade them to purchase more online, 53 percent of them cited more secure payment options. Payment security was chosen over price or product-related responses by a more than 2-to-1 margin.

So, there are major concerns about security online, so we thought we would step up to that concern, and focus on online security. Some internal data from Visa indicate the extent to which, from our internal perspective, security is important.

According to one of our Visa databases, in the third quarter of 2002, electronic commerce accounted for about 6 or 7 percent of all our sales, but it accounted for 15 percent of our fraud losses, and 23 percent of all

our chargebacks. Now, that's by dollar volume for those who keep track of that kind of stuff.

More figures that indicate the extent of the problem, in face-to-face transactions, only $.09 out of every $100 in sales was subject to a chargeback. That's for all of our volume.

For mail order, telephone order, it was $.27, and for electronic commerce, it's $.50 for every $100 was charged back. If we look at that from a transaction point of view, the trend is the same, 2 out of every 10,000 face-to-face transactions are charged back. For mail order, telephone order, the chargeback rate was 27 out of 10,000, and for electronic commerce it was up to 33 out of 10,000.

In the chargeback area, 71 percent of the electronic commerce disputes are cardholders alleging that they didn't do it at all. It wasn't that they didn't get the product that they ordered, or it wasn't what they wanted, it's, "We didn't do it at all." So 71 percent of our chargebacks are people who claim that it was someone else using the card, or they didn't do it, or whatever.

So, it's important, for our point of view, to have an electronic authentication or verification system. We think it will motivate a lot of non-shoppers to become

involved. It will reduce the chargeback and dispute numbers that we have got.

How does the system work? The way it starts initially is on the consumer side. Consumers have to sign up for the program. They can do it in a number of ways. When they open an account with a card issuer, they can sign up for Verified by Visa, and get their PIN number at that point. They can do it by going online to the issuing bank, and there is a process they can go through where they provide certain identifying numbers and information and get their PIN number at that point.

There is even a mechanism for doing it while they're shopping online. When they come to a merchant's website that is using Verified by Visa, some of the merchants have chosen to try to motivate using Verified by Visa by activating the Verified by Visa service at the point of sale. So, that's the first step. The card holder has to be involved in the process; it's his choice.

The merchant has to be involved in the process. They have to install software on their system, and the software has to meet the configurations and the standards set up by Visa to work.

But once that is done -- the cardholder has the PIN, and the software is installed on the merchant's site

-- it works in a reasonably transparent way for users. They go through the normal process of making a purchase online. And when they're about to actually make the payment, they then enter their account number.

At that point, a pop-up box appears, and they are asked to enter their PIN number. There is also a message that they previously recorded that says something like, "Hello, this is really Verified by Visa." It's a security feature that is put in there. But that pop-up box really is the opening of a communications channel between the cardholder and the cardholder's bank, the issuing bank.

The PIN number is inserted, there is a comparison between the PIN number and the account number. If they match, a notice is sent to the merchant that there is a match, that the person has been verified, and then the transaction goes forward as normal.

It's important to notice that the -- and as part of that transaction, the PIN number is not transmitted to the merchant. The PIN number goes to the issuing bank, it does not go to the merchant. You can't have fraudulent merchants setting things up and collecting PIN numbers.

How is it working? So far, we have to get a sufficient number of merchants signed up and a sufficient

number of card holders signed up so it makes sense for everybody. The Verified by Visa system is already up and working within the U.S.A. Visa-net. It's also installed and working internationally. All of the major processors of Visa systems are involved, and ready to work with it.

Nearly all of the U.S. issuers have implemented the Verified by Visa, or will do so in this year, and new merchants are coming on board and participating. The list of people -- we have Dell, who is one of our early adopters of the system. We have Disney, we have CompUSA, we have Orbit. Playstation.com is on board, Travelocity, JetBlue, more and more of the merchants are beginning to use the process.

It is a chicken and egg situation, where you have to motivate merchants to want to do it, and you have to motivate card holders to want to do it. It has to happen more or less simultaneously for the system to actually function.

For Visa, we have a lot of stakeholders in our system, and all of them have to get something out of a new product or service, otherwise it doesn't happen. For card holders, the advantages are straightforward. It authenticates their identity, it increases their confidence in shopping online, and it reduces the risk of unauthorized use of their card.

For the merchant, they get more consumer shopping protection against fraudulent use, and reduced dispute and chargeback incidents. For the issuers, for the banks that work with the card holders, they are comfortable that they are able to identify the card holder in these circumstances. They get increased sales volume, they get reduced fraud and dispute expenses.

The merchant banks, the acquiring banks in our system, they increase their sales volume, they have lower operational costs. All these disputes cost them money, too -- and this goes for new merchants in their system, as well. It's easier for them to acquire merchants.

So we think it's a product that has got some advantages. We think it's one of the tools that consumers will increasingly use on the Internet to protect themselves and to protect the information that they provide to merchants while they're shopping online.

MR. SILVER: Thanks, Mark. Let's discuss one final specific technology before moving on to some more general questions.

Many of us probably used these in the subway this morning. They are in our cell phones, and we also use them to access our offices. I'm talking about smart cards, of course. And Michael Willett has some remarks about them.

MR. WILLETT: Fasten your seat belt. This is going to be a fast tutorial on smart cards in the context of identity management and also a few current events that relate to smart cards.

Smart card, we're all familiar with this form factor. There are a number of other form factors, the most prevalent form factor is, in fact, a SIM card that fits into a cell telephone, mostly in Europe, and is used to provide identity management and credentials in the cell phone context. But this is the one we're familiar with, it's a little portable computer. Highly portable, highly secure operating system, data processor, et cetera.

Various form factors, I mentioned the SIM card, the slim credit-card size card -- this can be in the form of either contact or contactless. In the contactless case, it's used for access to buildings. Wave it in front of the little RF signal, it picks up the passive chip in here and does a little compute with the chip and verifies your identity, and in through the building you go. Or there's Easy Pass down the highway. So, there are various form factors.

There is a lot of physical and logical security built into smart cards, and it's improving every day. The one point I want to make here is that, in fact, the

way it's being used largely in applications is for securing and carrying and making portable your credentials. That is, the sum total of all the credentials that profile you, that's your identity, and I can carry my identity, then, in a portable fashion on a smart card.

A lot of services are available for smart cards. As I say, there is a little computer in here; most of the cards now are moving up to 64 kilobytes of memory, and lots of compute power. I can do data storage, authentication. I can do what's called multi-factor authentication.

That is, I have PIN access to the card. I may have biometric access beyond that. I may have challenge-response protocols that are handled by the smart card, so I can combine multi-factor authentication to provide strong authentication.

Cryptography is performed, digital signatures. It's an e-wallet, I can carry money in electronic fashion, I can carry, as I say, my profile for my identity management support. In more sensitive environments, I can have a shared intelligence between the card and a smart card reader that can be smarter. And so, the combination of the two can create a trusted environment.

Lots of applications. After issuing the card, I can still create applications that are new and downloadable to the card. Lots of advantages. One I will focus on here is privacy. That is where I put the control of my identity, of my profile, in the hand of the user. And through multi-factor and strong authentication, I have strong controls over the issuance of that identity. And each application can be designed so that it only accesses the minimal information needed for that application out of my sum total profile.

We have combined physical and logical bridging here between the physical world and the logical world. In some smart cards, hybrid cards, I can have pictures, I can have holographic images that make it hard to duplicate, like changing the color of the money from green to some off-green thing that we're doing with $20 bills.

I can embed the public and private key pairs with a public key. Lots of other credentials can be stored. I can imprint my driver's license on the card. There is a debate about whether driver's license should be a smart card or not. The American Association of DMVs is going through a harmonization exercise, and there is obvious resistance to using a smart card for a driver's license.

There are a number of hybrid uses. I could even put a mag stripe on here, and a holographic thing that could be read by optical readers.

Public key. Here is a very fast tutorial on public key. Alice creates two keys, F and G. F is public key, and that's published through a directory. G is kept private and secret. Bob wants to talk to Alice. Bob uses the public key to talk to Alice in coded messages, and Alice can be the only one that decrypts those messages using the private key. Alice, in theory, is the only one that converts ciphers back to messages.

Both those channels -- that is, the publication channel for public keys, and the cipher channel -- are available to eavesdroppers. So I can see, as a bad guy, both channels. My challenge then, which mathematics says I cannot do, is to recover the private key. I want to guess Alice's private key, knowing those two channels.

Now, the only thing missing here is that I want to make sure that Alice's public key, F, can't be spoofed by someone else imitating Alice. And so Alice does a registration process with a certificate authority, a well-known entity, trusted entity -- in some places, even the Post Office, in some countries, that is -- and the well-known entity, the certificate authority, certifies a copy of Alice's public key for distribution.

Two ways that smart cards enter into this picture. In confidentiality, for encryption, follow the bouncing ball here. Bob downloads the public key of Alice from the public directory. He encodes the session key that he wants to use with Alice, sends that to Alice. Alice uses her private key -- the only one that can do that -- to decode the session key, and then the two can use that shared session key over a public channel to do regular high-speed encryption.

So, the smart card, carrying Alice's private key, can do that deciphering step all in a trusted environment.

If I apply a public key in reverse order, that is, and let Bob apply his private key to a message digest that creates what's called a digital signature, Bob is the only one that can do that, in theory, because he's the only one in possession of the private key. Alice can retrieve the public key of Bob from the directory, and can decode, in a sense, the message digest, the signature, can convert it back into what it was originally, and compare to make sure that nothing in the message was altered.

So, by applying in an elegant fashion -- the private key first, then the public key -- we have a digital signature concept.

All of these things that I have described quickly here can be combined on a smart card. I can do the PKI, public key infrastructure stuff, I can store certificates, which are the certified copies of public keys, I can do the computation related to public and private keys, I can do the encryption, I can combine this with biometrics -- that is, I can use either facial geometry or fingerprint or iris scans, or handwriting dynamics, that sort of thing, I can store the minutiae for fingerprint, and do the local checking of identity, of biometric identity, locally on the card, as opposed to back at some central point.

Why have smart cards then, if they are so good, not been picked up in the United States as rapidly as in Europe? Even though we're coming on strong in the United States, as you will see by current events.

And I borrowed this chart. I have no idea why that person is doing that smoke thing in the corner. Must relate to this chart, somehow. Here are a few reasons why.

First, we have this neat little telecom system over which we have been exchanging credit card numbers for many years. Traditionally, until recently, we had very low fraud rates. But what you have already heard is that when we have card not present, or card holder not

present, these fraud rates go up dramatically.

No government-mandated card. I will say "yet," that's a personal observation. No government-owned telephone company. Should I say "yet?" And we don't have a health card, national health card system yet, either, in the United States. So those are some of the traditional differences between the Land of the Free and Europe that have, I think, impeded the growth of smart cards, but they're coming on strong.

Any of these market surveys, here is the latest one, it shows tremendous growth in all of the form factors, and all the dimensions for smart cards. And there is a good one you could -- I have given the website at the bottom, here -- it's a very good annual survey from Schlumberger, one of the smart card providers. They do an annual analysis of the marketplace, and I just extracted a few highlights from that.

SIM cards in mobile communication and telephones are still strong, but we are seeing the 64-kilobit cards coming on. Travel -- the contactless smart cards for access and travel are increasing by 25 percent. And JavaCard is getting to be the predominant operating environment for smart cards.

Going on this week is the largest, I think, and most attractive annual show in the United States for

smart cards, the Cardtech Securtech meeting going on in Orlando. That's why you have me. I think I'm the only guy in smart cards that couldn't afford the flight.

And here are some of the topics, some of the workshops that are going on there to show you what's being highlighted. Biometrics, anti-counterfeiting, contactless biometrics, and so on, and interoperability. Big issues.

The Department of Defense is now distributing what's called a CAC card, the common access card. It's to be ultimately used in all the military for personal identification -- that is, for storing your profile, access to buildings, and applications, encryption, digital signing, e-wallet functions, and medical data.

As I say, it's being distributed across the military now. Ultimately, 4 million cards will be distributed in the first wave. And there is a very simple -- this is nice about the issuance of such a large number of cards -- there is a very simple initialization issuance system based on two systems, called DEERS and RAPIDS, for distributing these cards.

At the same time, NIST is involved in promoting an interoperability function specification called the GSC-IS, the government smart card interoperability spec.

The problem, historically, is that applications

have been hard-welded to -- readers have been hard-welded to smart cards in a vertical proliferation of market. And so that's bad, right? Too many parts, and I want this part to run with that part.

So, the interoperability spec has introduced a grammar and some interfaces that will allow applications to uncouple from given smart cards, if you will. And so, NIST has been promoting that in not only the United States, but has gone on a grand tour here recently of Europe, trying to promote this spec.

The homeland security people are going to pick up on the CAC card, and are going to distribute it even further. There are some highlights about that. JavaCard, they're going to add memory. The current CAC card is 32 kilobytes, and they're going to add a little more memory, 64 kilobytes.

They're going to make a two-chip card, so that I will have a contactless card in there that allows building access in this version. So this is a big roll-out in the United States, based on the CAC card.

There is a group called the International Civil Aviation Organization, ICAO. They have just recommended, in Montreal, in fact, that facial recognition and contactless smart cards be combined so that I basically can put a smart card in a passport, I can smile into the

camera, and pass my passport near the reader, and the comparison can be made between my facial geometry and the stored image, just like you would be doing with a fingerprint. They like pictures of people better, because we're already having our picture taken, instead of being fingerprinted.

The United States, by the way, now coincidentally, is also requiring by October of next year that all foreign nationals entering the country will present travel documents with some form of biometric data. They also said they would endorse whatever the recommendations are of the ICAO.

So if you put transitivity together it tells you that the United States, by October of 2004, if all this time line falls in place, will require facial recognition contactless cards in passports. Just another form factor.

And finally, what's going on in Europe? In Belgium, they are rolling out a national identity card that will contain tax return information, change of address, civil records. It will provide access to all of those, it will contain some personal information, health care information, and so on.

Ultimately, the rollout is to 11 million citizens in Belgium. Same thing going on in Italy, so

we're seeing smart cards used in the identity management context.

In summary, what I would say is some of the strengths of smart cards in this identity management context are I have multi-factor authentication, mainly I have my profile, my personal information, in my control, especially given that applications are cryptographically portioned in this smart card to only access minimal information needed for a transaction. Thank you.

MR. SILVER: Thanks very much, Michael.

(Applause.)

MR. SILVER: Let's move now to some general discussion questions, and I want to pick Alan Paller's brain, first, with this question. Are the tools we have discussed so far sufficient to help consumers protect their information security?

MR. PALLER: Hardball, huh?

MR. SILVER: That's right.

MR. PALLER: Let's grade them a little bit on two criteria. One is are they transparent? I think Rich Lloyd's word is exactly the right word -- or Toby uses another term called "security baked in."

And we know, from panel one, that if they're not, they're pretty much irrelevant because if they're going to make everybody do a lot of work to use them,

nobody is going to use them. We have got hard data on that, and we know that's true. So that's A.

And B is do they do what the consumer thinks they do? Meaning, do they actually protect? So, I hate to do this to Mr. Smith, but his favorite kick-off was SSL, and SSL clearly wins on the first one, right? It's built into everything, we all know. But does it actually do what the consumer thinks it's doing? It gets an F on that.

Do you know why? Because although SSL protects your credit card information as it flows through the network, when it gets to the place where it's going, the company that put it there bought some out-of-the-box Microsoft web server and stuck all your credit card information on there, ready to be attacked, and no criminal is stupid enough to attack your home computer when he can collect millions of your credit cards from the vendors that do e-commerce with you. Which is why one of the things that Mark didn't talk about, but I think is one of the really big things that's a winner -- and I know we're going to talk about that in the other panel, I mean, in the other workshop -- is that they have a program that forces the merchants to encrypt the data.

If the merchant doesn't encrypt the data, you've got no sense in sending your credit card there.

Now, you don't care, because the merchants actually have to pay for the losses, but it's really a pain to have your credit card stolen, and have to go clean up after that. So you care enough that you don't want to do business with vendors that don't meet Visa's minimum requirements.

Second one we ought to give a grade to is the anti-virus tools. They get a very high grade on effectiveness, A-minus. The only reason they don't get a higher grade is that they miss all the new ones, right? I Love You got through because it got through before they had the profiles out. But they get a D or so on adoption, the Dell data gives you that data. They're just not being used, because they're not transparent, they're not built in, they're not baked in, so they're a wonderful tool if we used them, but we don't use them. So they don't get a high grade.

Even more so with firewalls. Firewalls are very effective, but they're not built in, and they're not transparent.

I think that the most useful thing that's happening here, in terms of tools that work, is something that actually Dick Clark was the godfather of, and Howard Schmidt did a lot of the follow-on work, which is the development of consensus standards. We're not going to

have government-mandated standards for security.

But they created something -- they helped create something back about two-and-a-half years ago, which was a gathering of federal agencies and big companies. Boeing, and Mrs. Fields Cookies, and Intel, and lots of companies got together to agree on what safe computing was. And because they did that, Dell was able to deliver out-of-the-box safe configurations.

And just to put that in perspective, do you remember Code Red, and how it infected lots and lots of people? Most of the people that it infected didn't know they had the software that was vulnerable, because the vendor had stuck that software in and turned it on without the buyer of the software knowing. And without consensus benchmarks, there is no way you can get users to configure the system safely.

So, I think the really high grade for this panel goes to Dell, even though it's the newest one, because they're doing security baked in that protects us.

The other grade that we will give is a Gentleman's C to Microsoft. They get As -- in fact, we're going to give them two of the security leadership awards in the summer -- for spectacular new things. But they get raw Fs in some other areas, and I just want to mention a couple of the raw Fs.

They have just come out with security benchmarks built into Windows 2003 server addition. But you can't buy an end user system with security benchmarks built in for Microsoft. You have to go to Dell to buy it, and you can't do that yet. But some time --

RICH LLOYD: Not ready quite yet, but we're getting close.

MR. PALLER: Some time shortly you will be able to do that. That's an F. Does that make sense? If they know enough to serve up the large companies, they ought to be doing it for the small -- for the other companies.

And the other one that Microsoft gets an A and an F for, is if you get XP, Windows XP, and you go through the installation script, they get an absolute A, because it asks you, "Do you want to have patches automatically delivered to your computer," and the default check is yes, as opposed to the default being no. The default check -- I know this is not okay to the privacy people, they want opt in. But this is one case where we like the opt out strategy.

So they give it to you, but they made a corporate decision not to do that for all the hundreds of millions of computers that are already out there. Now, I'm not looking for it on Windows 95, but Windows 98, Windows 2000, it's absolutely silly not to provide that

same kind of service, if only to charge us $10 a year, the way the anti-virus guys do.

MR. SILVER: Thanks, Alan. Let me pose a general question to anyone who wants to take it up, which is this. What incentives are needed, and also, which incentives already exist to develop new consumer tools for protection of information security?

MR. WILLETT: Well, if we just see what's happening in the web today, you will see the evolution, from browsing to information transfer, to what -- the big hot button these days is Web services.

And so, I think the incentive is there, by brute force. That is, we're going to be starting to see value transactions. That is, things that have real value, real monetary value, real intellectual value, exchanged more and more through Web services.

Standards are being developed in this area, the Oasis Standards Group, for example, is developing all sorts of interoperability languages using XML, and so all the ground work for Web services is being laid, I think, correctly. And so, Web services are going generate value transactions, a forced incentive for us to develop better privacy controls and better security controls in that environment.

At the same time, companies -- so many

companies -- are basing their life blood on their trust image, on their branding images. So I think there is a lot of incentive, from the business side, to be good citizens in the web services environment, because of the branding.

MR. MACCARTHY: And if I could just jump in, from Visa's point of view, the incentives are for us to promote good security practices on the Internet. I want to thank you for your kind comments about Visa's card holder information security, and for those of you who want to hear more about it, there is going to be another session on business tools, and the card holder information security program on June 4th. So, it's not the one that I will be talking about in this program.

But for that program, and for the Verified by Visa program, it's Visa's interest in promoting online commerce that is driving what we're doing. It has a good effect for consumers and for businesses, in promoting security online, but the motivation is, in part, promoting the brand, and in part, good corporate citizen. But in large part, it's promoting a channel of commerce in which we have a serious financial interest.

MR. SILVER: Larry Clinton?

MR. CLINTON: Yes, I would like to divide this into two different sections, one of which is what Mark

just spoke to, and Visa's a member of the alliance, and we're delighted to have them. They're one of our great examples.

We have some other corporations who are doing similar sorts of things. Nortel, for example, who is attempting to take their security needs and expand them out to their vendor community. And I think that profit motive is going to be the prime incentive in finding model instances such as Visa's -- to provide some sort of economic incentive for the current adult population.

And the business community, I think, is another thing, and I am joining Mark on the business panel, and we should go into that there, because I think there is a trickle-down effect.

But the second area that I think is really critical -- and I congratulate the FTC, and we have done a lot of work with Orson Swindle and Dan Caprio on this terrific stuff -- is the creation of the culture of security. And for that, what we need to do is talk about finding the incentives for our school systems to start teaching the sort of behaviors which will transcend the technological advances.

I mean, my daughter now comes home and is vehemently anti-smoking, vehemently anti-drug. I have an autistic son. But if I get in the car and don't put my

seat belt on, he screams at me, "You put your seat belt on now." Those of us who are my age know that, it used to be nobody would put a seat belt on. You know, a violation of our rights, and everybody smoked.

Not true anymore. We can change these cultures of security, but this is not being done, to my understanding, in the school system now. We are putting computers in all the schools, but we're not teaching kids cyber citizenship or cyber security. And I think that we need to have some sort of hand-in-glove situation so that when we have programs to get the school system connected to the Internet, which is a wonderful idea, and get computers in the schools, we also give them cyber citizenship, cyber security curriculum, because we need to grow this culture of security from the ground up.

MR. SILVER: Thanks. Richard?

MR. SMITH: Yes. I think the main incentive for the home user of getting better security in the products that they buy are actually incidences. I can just go down each one. If we look at Microsoft Word, it has better macro-virus protection in it, because that problem got out of hand.

We had Outlook Security Update come out after -- the first one after the Melissa Virus, and then we learned that wasn't good enough, and then the second one

was after the I Love You virus.

So, we have the CD universe case, which has driven more on the business side of protecting websites and information. That's all very reactive, and I think that's unfortunate. But it's going to be much better if we were more proactive about things.

I do think that Microsoft, being the primary vendor of software that we use in the home -- however, now, is being more proactive. We, unfortunately, have to wait two or three years for it.

I also share Alan's view that it's unfortunate that the older versions of Windows aren't being retrofitted with some of these same kind of security protections.

MR. SILVER: Thank you.

MR. PALLER: Can I throw something in?

MR. SILVER: Sure. Before you do, those of you with questions for the panel, if you would go ahead and line up at one of the mics, and we will take questions right after Alan Paller.

MR. PALLER: I love the idea of getting to the kids early. In fact, Governor Ridge and the Stay Safe Online Program at SANS annually has a poster contest for the kids, and they come to the White House, and they get prizes, and it's a wonderful idea.

It ain't going to change. It is absolutely essential, we must do it, but it isn't going to be even a bullet, a silver bullet. It's necessary, but absolutely insufficient.

I think a more important feature that earns another A for Microsoft in Windows 2003 -- it has the Nancy Reagan feature, the Just Say No feature. It has a feature that doesn't allow you to connect your computer to the server unless it has minimum anti-virus settings and firewall settings and other settings -- I don't know all the settings that are controllable.

But without that kind of technology built in, I don't think we're going to win just on the training, just the way we can't win safety in driving just by teaching kids safe driving. We also have to build safer cars. And it seems to me we need to build safer computers, and things like that Nancy Reagan feature help.

MR. SILVER: Thanks. Ari, were you first in line there?

MR. SCHWARTZ: Our part of the room is interested in -- and Ed Felten and Marty both raised similar questions to what I have, which were about smart cards. And Alan didn't give a grade to the smart cards, generally, and Rich didn't talk about building smart cards readers into the PCs.

It seems as though if it's going to catch on, it would be baked in, you're going to try security in that kind of way. I mean, obviously, there is still some security card work that still needs to be done on the smart card side. But in terms of the readers --

MR. WILLETT: Well, Dell is, of course, shipping -- there are a number of vendors that already sell card readers with integrated smart card readers in the keyboards, so that the whole keyboard becomes a trusted environment. And Dell is now shipping one of those as a base system.

MR. LLOYD: Yes I should have mentioned the smart card reader system, and I appreciate the reminder. We do see pretty good demand for the integrated smart card reader, although again, not the demand we would like shifting down into the consumer segment, which is the topic of discussion today. And the reasons for that have been well enumerated.

There is also a lot we are doing, from a middleware and a USB smart card reader perspective, in terms of bundling in the hardware. So, this is something that, like everything else, we're balancing the economic reality of demand for these things, but also trying to be at the forefront of the supply curve, putting these things out into the market.

MR. SILVER: And --

MR. WILLETT: You can actually have smart card readers integrated with keyboards with biometric readers on the keyboards. So the keyboard is getting to be a piece of intelligence, all by itself.

MR. SILVER: Next question?

PARTICIPANT: We want a grade, though.

MR. PALLER: You want a grade? You get a C, coming up for built-in, you get an A for effectiveness on one dimension, which is that it is the right way to keep people you don't want out of your systems. Having something that they have in their hand to get on the system, rather than a password, is absolutely essential.

All of us are moving to it. But it gets to the same problem as SSL, doesn't it, Ari, that at the other end, the credit card data is in an unencrypted database.

MR. LLOYD: And one thing I would just say, and you know, you hear this message from a company like ours a lot, but really, standards-based computing is what will help drive some of this stuff.

So, if you want to go back to the previous question, what are the incentives, well, the incentive -- to expose my private sector stripes even more -- the incentive is the creation of value. And the value gets created as standards are put in place, as Alan said, and

those standards make it easy and affordable for companies to provide widely accepted, widely standardized technology easily, cheaply to the masses, and then it gets adopted quickly.

And that's what we see with an example like Verified by Visa, where the creation of value is there. It's easy for a merchant to do it, because they make the money back in the shrinkage loss and in the chargeback loss. So it's a win for the company, it's a win for the consumer, and it's a win for Visa. That's the kind of program we have to have.

MR. PALLER: And they don't have to be government-mandated.

MR. LLOYD: No, it doesn't.

MR. PALLER: The Center for Internet Security showed, with Dick Clark and Howard Schmidt, that you can do it with a consortium of federal and consumer organizations and industry groups, and it doesn't have to be federally mandated.

MR. SILVER: Let's take another question. Does that mic work over there?

MS. BAUR: Yes. Hi, I'm Cynthia Baur, from the U.S. Department of Health and Human Services, and we actually have a national public health objective to increase Internet access in the home, and we're also

working on this concept of a national health information infrastructure.

So, from that perspective, I'm really interested in this idea of what consumers or patients or just people searching the Internet for health information, for example, could be expected to do and know.

And I would like to ground this conversation a little bit in the demographics of who we know has Internet access. And so, if we look at who is currently on the Internet, it's still higher education, higher income, and associated with that, is higher literacy. And along with literacy goes the ability not only to read, but to understand and do higher order thinking and understand things more abstractly and conceptually.

So, I am really interested in this idea of what it is that people can realistically be expected to understand and do, especially if I'm thinking about it from a public health perspective, and the flow of health information over the Internet.

So, I would just like to hear the panelists' comments on that, based in the demographics of Internet use.

MR. SILVER: Any takers?

MR. PALLER: Sure. Two threats. One is I will

get wrong information, and two is I will have bad things happen to me because I go somewhere where I shouldn't go. There are probably more threats, but let's just deal with those two.

If I am concerned about getting bad information, then we move into standards for -- just what Rich Lloyd was talking about -- standards for the websites I go to, and some testing method that I can be sure that they have their systems configured safely, according to some benchmarks.

And if we go to "I'm getting infected because I go there," that's solved by a re-engineering of the operating system. Microsoft has known how to do that for at least seven years, they have just consistently avoided doing the work that they need to do to make it possible for me to go to a website, and if the website is not known to be on the FTC's trusted list, then I don't allow that software to get into my operating system and screw me up.

I'm sure there are other threats that you want, but I don't think education is going to help if a person is worried about whether their kid is going to die of cancer. This whole idea of safe use of the Internet -- education just isn't going to be the solution.

MR. SILVER: Stephanie?

MS. PERRIN: Yes, Stephanie Perrin. I've got actually two questions, if I can. The first one is what do you think the impact of some of these privacy and security tools is going to be on trust in the consumers?

Example, I now run Microsoft XP -- sorry to pick on you guys again, Richard and Phil -- and I have configured my firewall to block everything going out, or at least alert me so I can make a choice.

Well, having worked at Zero-Knowledge Systems, it's not like I'm unaware of how buggy Microsoft's software is, but I am truly staggered at how often I get told that Microsoft is trying to talk to itself. And this makes me nervous.

And I am not a geek, definitely not a geek, but I am not a neophyte. So if I am nervous, what about the grand public out there. That's my first question.

And my second question is -- and it's similar to the SSL A and F problem that was brought up a minute ago -- with the smart cards. First you've got a problem that you really didn't address, how do you get beyond -- and I'm not suggesting you should have -- how do you get beyond the user acceptance, or the concept of an identity card. That's a big one.

But secondly, the threat scenario moves to the readers. How do I, as a user, know when it's safe to put

my card in a reader, because there will be people getting me to put my card in readers so they can run off, hack my card, get into the data, et cetera, et cetera. Right? Do we have any readers out there?

What kind of problems do we get into with wide scale deployment of smart card systems?

MR. WILLETT: Just a comment, and a mention of Microsoft there again, too. If you follow the Palladium initiative, and what's called TCG, Trusting Computing Group now, and TCPA, and all those other acronyms, in the whole industry there is a real shift toward moving trust and trustworthiness to the client side.

So there is a real focus in the industry on offloading the security from servers -- or at least balancing the security on servers with the client. So that's a general push.

And I think the other thing to do is just watch what happens in Belgium, or Italy, or one of these countries that's rolling out national ID cards with health information and so on, and they're having readers in the home, in kiosks, in public buildings, et cetera, massive deployment. It's just a matter of -- there is a practical environment in which the test limits, the system design of such a design.

But again, in technology, we are pushing toward

client trustworthiness, and we're rolling out systems today that should have the right safeguards built in.

MR. SMITH: Yes, I would like to address the firewall question. I think this has already come up. Firewalls are more -- of all the security products out there -- are one of the harder and more techy products to use.

And what you're pointing out here is, on one hand, you've got Microsoft XP phoning home to do an update, which is a good thing, and it's doing it a lot. So maybe there is a trust issue there. What is it really doing?

And a firewall really doesn't tell you that, it's just operating at a low level. So at some level, if you're going to use a firewall, it's going to require a higher level of training, I think, than some of these other products, unfortunately.

MR. WEITZNER: Thanks. I just have a question. I want to press any of you who are willing to be pressed on how we're really going to see more consumer individual user-level security -- and privacy, but I will -- we can leave privacy out of it for now.

And it's based on an observation that if you look at where security is actually developing, where there is actually progress, where Alan's grades average

above a C, as opposed to below a C, it does seem to be in what are basically centralized and large, but effectively closed networks.

So, I think, obviously, what Visa is doing is terrific. A lot of what banks are doing, the military is doing -- these are all centralized communities that are able to make top-down decisions about doing security, and able to push them, I think rightly, and say, "We're doing this now, guys, because we have a real problem."

And I look at the other side, the consumer side, and frankly, the Web side, including the Web services side, and these are decentralized networks where there ain't no one, including W3C, Oasis, or anyone else, who is able to say, "Okay, guys, we are doing it now."

As the gentleman from Dell said, certainly there are standards developing at W3C. We have a lot of the foundational XML security standards. Those are gradually being picked up into Web services, but I would emphasize the word "gradual."

And I just wonder what your thoughts are about whether -- well, I guess I want to express a note of skepticism about whether it's enough to say the market will sort it out for these consumer-level services. I believe that's the case when Visa has its network to worry about. I believe that's the case when the military

has its network to worry about. What about the rest of us, is the question.

MR. CLINTON: I appreciate the question, Danny, and I think the answer lies in segmentation. You know, there is a certain segment -- the early adopters, the current users, the people who are not geeks but know all about how to use a firewall and don't think they would be classified by the general population as geeks, with all due apologies.

I'm not so worried about them. They're going to read stuff, they're going to get on the Net, they're going to investigate, they're going to adopt the best available technology. They can afford it.

And then there is -- if I may go back to my education pitch. Stay Safe Online and a picture program at the White House are not what I'm talking about.

I'm talking about if you want to adopt a culture of security that is going to be part of the entire population, we've got to get them young, and I'm talking about curriculum taught in the schools. I'm talking about reading, writing, and computer skills and ethics as part of our general curriculum. That's where we're going to get this. Because the technology is going to continue to change. Now, those are the two extremes.

There is a big segment in the middle, which is

kind of us in the room, that I think is the more difficult segment. And I think, for them, you're going to need a whole variety of things. I agree that most of what we're talking about are the closed systems, and that's pretty much what I deal with at the security alliance.

I guess our best hope for this is the trickle-down effect, that we are going to be able to have good education programs -- and again, going to the next workshop session -- one of the things we're going to be talking about is incentives for businesses, and one of the things that we're finding out is that the most cost effective of all the security interventions that we're finding in the business community is training programs.

And we are hoping that when we train people in the Visa corporate network, they're going to go home and be individual consumers at home, and they're going to say to their husbands or wives, "Don't do that," "Don't download that."

So, we're going to have to have a messier way to get to that middle segment, and I don't hold out immediate hope. I don't think there is a silver technology, or a silver bullet anywhere. But that's the segment that's going to be tough to get, and I'm not sure we're going to get all the way there.

MR. SILVER: The last word goes to Anson Lee.

MR. LEE: Yes, definitely awareness and education is a key to this. And the government has a definite role to play. Because when we, as individual corporations, try to expound upon Internet security, they look at Symantec and say, "Oh, they're just trying to sell product." But when you have the government saying, "Well, this is what it takes to be secure, or to be a good citizen on the Internet, and these are the steps that you can take, go ahead and take a look at the tools that are out there and go ahead and make your own decision," because when you know what is actually going on you can make a better informed choice of what is right for you, as you are sitting at home in front of your computer, doing what it is you want to do on the computer.

MR. SILVER: Well, we have consumed 10 minutes of lunch time. But please come back at 1:00 for panel 3, and I want to thank this panel for a very informative discussion.

(Applause.)

(Whereupon, at 12:11 p.m., a luncheon recess was taken.)