TRANSCRIPT

PROOF POSITIVE:
NEW DIRECTIONS FOR ID AUTHENTICATION

PANEL 4

APRIL 23, 2007

>>AVIVAH LITAN

Hi, I just wanted to point out that the session starts at 2:15. The printed schedule says 2:00, but it ended up that we're starting at 2:15. So just in case you're wondering why we haven't started yet. All right. Thank you very much for cooperating with the delay. And we will begin now with our next panel.

Thank you very much for coming back from lunch to hear about authentication technologies. Quite often, people mix up identity proofing and authentication. We've heard about identity proofing in the previous panel especially. And, assuming that you know who you're dealing with, then you give them an authentication credential. So we're talking about after you've proved the identity, now you want to give that person a credential so that when they come to your branch or they come to your Internet site, they can prove that they are who they said they were when they enrolled. So authentication is different than enrollment and identity proofing, although they go hand-in-hand.

We're gathered together with a very distinguished panel that represents all the different gamuts, not all of them, but many different gamuts of authentication technology. And we'll hear from each of them and then we'll open it up to questions and hopefully you'll participate. You can interject at any point after the presentations. So I'm just going to run through the panelists, their names and titles, but their bios are in the handouts if you want to learn more. On my immediate left is Victor Lee. Victor is a senior consultant for the International Biometric Group and he'll be discussing the different methods of biometrics. To his left we have Phillip Hallam-Baker who is a principal scientist for Verisign, for security at Verisign. And then next to Phillip, we have Neville Pattinson to talk about Gemalto and their perspective. He's Vice President of government affairs and standards. And then to his left is Marc Gaffan from RSA Security, which is now the security division for EMC. Marc is director of the consumer solutions business unit. And to his left is Micheline Casey, who is senior director of identity management at ChoicePoint government services. So we've got biometrics, we have PKI and SSL security, we've got risk-based authentication, we've got smart cards, we've got knowledge-based authentication -- all that knowledge is here on the panel. So we'll start with Victor and he'll give us a short presentation.

>>VICTOR LEE

Just to see if you're on your toes after lunch, if you can identify which one's actually mine. All right. Here we go. So, first, I'd like to thank the organizers for inviting me and for

me to have the opportunity to speak to you about biometrics and identity theft.

Just a quick little blip about our group -- International Biometrics Group -- so you'll understand the [?]from which I'm coming. We've been in the biometrics consulting integration and research area for over a decade now, and our main claim to fame is basically that we take a very vendor-independent and technology neutral perspective. Hopefully anything I say is coming from the heart and is true and is not necessarily coming from the fact that we're biased one way or another. I know that that bias word has been hammered at earlier today. So you can read this at your own leisure. But basically we have experience both deploying systems, understanding how they work in practical environments as well as doing the research to understand what the context is for these technologies, what actually exists in there and also to understand what sort of opportunities might exist for these technologies in the future which brings me to the issue that we're talking about today.

One of the important things that I think we have to understand before we talk about biometrics is understand what exactly are biometrics? A lot of people say we understand what these are, we've seen Gattaca, we've seen movies on Hollywood. It's those fancy technologies out there that are really cool and new fangled. Yes, they are cool, new fangled; they are pretty awesome. But there has to be some formalized concept so that we can begin to talk on the same level plane.

Basically the formal definition we have is the automated measurement of physiological or behavioral characteristics to determine or authenticate identity. I want to highlight three major points here. First, that it has to be automated. We're not talking about somebody just going ahead and comparing a fingerprint against another fingerprint they have seen before. It's actually some automated process that already exists, some mechanical-based approach. Second has to be physiological or behavioral. And the third one is we have to make sure that it's geared towards determining or actually authenticating an identity.

Examples of these technologies, these are not all inclusive, but they give you some examples of what are the major technologies that exist out there. You have fingerprint-based technologies which perhaps a lot of us are most familiar with. AFIS-type technologies which are essentially automated fingerprint identification systems. These are systems that often deal with ten prints and are used in a law enforcement-type application. They deal with more images as opposed to, say, templates which the fingerprints operate with. Then you have the other ones such as Iris, facial recognition, hand geometry, voice signature, vein, a whole range of different biometrics which can be broken down into both physiological and behavioral components.

What we have to understand is that actually, no biometric is purely physical or purely behavioral. There's actually elements in both in almost every type of biometrics that exist out there. Even a fingerprint, which you might say, "this is such a personal aspect of me." Well, the way in which I place my finger on the device may confuse the system. And that is the potential way in which the system may have a vulnerability, something that we as employers have to concentrate on, have to think about if somebody is able to place their finger incorrectly or place their finger in a slightly different way so as to confuse the system, that might actually be a

vulnerable point on how a person could trick the system into believing they are somebody else.

Let's get more to the issue of biometrics and how they help. One of the main points that we had discussed earlier, or that some of the panelists had mentioned this morning is the issue of convenience. And oftentimes there are ways in which biometrics can be deployed to facilitate a process such as transaction. There is a company such as Pay by Touch which has been going around and their basic concept is let's utilize a fingerprint so that you can tie it to your checking account. When you want to go to the cash register, you put down your fingerprint, it automatically deducts whatever you purchased. No need to bring a card with you, no need to bring any type of other device.

But the trick with this is that convenience is going to be inversely proportional to security. When you try to move towards one that's a little bit more favorable of reducing the number of things that you have to bring with you, you may reduce the amount of security that you have available. And we have to be careful because there's a lot of times when security is often let loose as the result of trying to push people through increased through put, through again the payment solution, the payment terminal area.

Think about the last time somebody actually took out your credit card when you are making a purchase and compared that signature on the back. If you're like me in the last 20 years, I haven't had it done a single time. That can be an issue. You also have to think about what the potential problems are going to be if, say, people want to bypass somebody's security functions. If the easy solution is let's just prop a door open so we don't have to deal with the headache of somebody that doesn't authenticate themselves correctly with the biometric technology, you've got a problem. You've got increased convenience but you lost the security element that biometrics can potentially provide.

With biometrics, how can they help? As I was saying, the pay by touch, bio-pay type program, you don't have cards. There is nothing you have to physically carry. You don't have to worry about somebody stealing it. You don't have to worry that you might lose it. If you lose your finger, you have bigger problems on your hands than having to deal with issue of identity theft at this particular moment. And there is also one authentication credential. You don't have to worry about forgetting your password or substituting, or you could use your fingerprint to substitute for multiple passwords. If you're dealing with many systems, many different types of online accounts, you sign into eBay, you sign into a Yahoo type thing, use the fingerprint. Use some other type of biometric to substitute for every single one of those other potential authentication credentials.

Another thing that's also good but also a potential negative of biometrics is a lack of transferability. This could be beneficial if we talk about one of the topics brought up earlier today that you have predation. You have child predators who are essentially trying to take advantage of a site that may have been explicitly designated as being for children only. But if an adult is able to use their kid's pin, you have a problem. Likewise, if an adult is taking their child's iris, taking their fingerprint, taking their voice, taking their vein, again, bigger problems are at stake here.

We have to focus on distinct personal user characteristics; that's what makes biometrics very strong. It also is a way for enhancing the responsibility for the particular ID that you have. One of the actions, one of the projects that IDG has been doing is an independent validation of a program down in Texas where people who are trying to claim certain benefits, certain medical benefits need to use their fingerprint to designate that hey, they're the actual person there to whom the proper services should be issued. And it's also a way for the government to check and later on see whether or not the person who placed their finger when they exited – when they entered the system is the same person who places their finger when they exited the system and measure how much time actually took place between those two points. In other words, if you're getting a simple checkup for 30 minutes and you put your fingerprint down in the beginning, 30 minutes later put your fingerprint down when you're exiting, that surgeon better not be charging you for open heart surgery because they're going to get wind of that very fast.

Another reason biometrics could potentially be helpful in types of identity theft situations, is that criminals sometimes feel a deterrent factor as a result of something so personal, something that belongs so much to you physiologically, behaviorally. I don't want to leave behind my biometric it that could perhaps be linked to me ultimately when somebody is doing forensic analysis. So that kind of a deterrent can be a very effective means of or justification for using biometrics. Again, generally they're harder to transfer. They're harder to capture and steal. And phishing for biometrics is a lot more challenging. You've got to understand, as a gentleman said here before, there are images and then there are templates. Templates essentially represent little mathematical codifications of that image. The little subsets, if you would. Somebody's stolen templates cannot be reverse engineered. You could get essentially three points of a finger. You can't necessarily reconstruct a whole image of the finger based on just three points alone.

Another way is that you use templates and specific aspects of a biometric only for a specific core purpose or program so that if that gets compromised, you're not at issue with every single other program that's using a similar biometric. It's like taking different parts of the puzzle and using them, different pieces of a puzzle and putting them for different applications.

Also, biometrics have been utilized to help stop multiple registrations. When you have folks coming into motor vehicle registration points and trying to get multiple IDs, well you use the biometric device. That biometric device can be utilized to essentially say hey wait a minute, you've been here before and I can prove that this is the case. It can also be used when you're talking about check cashing fraud. Some folks have been using different names to try to cash checks and then run without being caught. Using a biometric can help limit the efficacy of that particular approach by linking it to who they actually are and not necessarily caring what their name is as far as that part is concerned but who they personally are. And, of course, biometrics can also be utilized, as I think more and more laptop manufacturers are discovering, for logical access restriction, whether it's swiping your finger on a Lenovo laptop, a Toshiba satellite. There are various different types of technologies out there. PDAs, even cell phones these days are able to utilize facial recognition, with the high resolution cameras that you find on your phones as well as fingerprint devices, voice authentication, things of that nature.

Now one of my major points today, my major point if you would, is going to be that

when you're talking about an issue such as identity theft, you're going to need a tradeoff between convenience and security, and I would personally urge a direction more in the line of security. What that means is let's try to aim for, what I call, the identification trifecta. By that I mean, we have, what you have, proximity cards, swipe cards, keys, fobs things of that nature. We've had things that you know. PINs, passwords, but now we also have this tool. Over the last decade we have developed this technology called biometrics that enables us to have not only what you have, what you are but also what you know. This combination of three very important factors, multi-factored solutions, if you would, can really lead to what I feel is going to be an efficacious counter identity theft system.

But we've got to be careful, and this is where I'll conclude, because biometrics are not a fool proof guarantee. We still have to use common sense; we still have to use good practices. What good practices may mean is you use multi-modality systems. You use many biometrics. Combinations of cross cards and fingerprints.

There are also privacy issues that have been raised several times already today. I would refer you to bioprivacy.org which details some of the practices that our company has developed as a recommendation for ways we can deploy systems effectively but at the same time with respect to the citizen, with respect to privacy concerns that exist out there.

And then there are issues such as spoofing and other vulnerabilities out there. Spoofing by which I mean somebody taking a fake finger, taking a fake iris, taking a spoof, if you will, a fake artifact to try to break into a system. We've got to be careful of that. The reality is biometrics are not fool proof as I said. We have yet to find a fingerprint system that we have not been able to break into in our organization. But that does not mean necessarily that the device itself is flawed. It just means we have to be careful about the particular contexts in which they operate. So I'll conclude with that remark.

>>AVIVAH LITAN

Thank you.

>>PHILLIP HALLAM-BAKER

Going to have to do this the slow way.

>> AVIVAH LITAN

We tried to put it in the right order.

>> PHILLIP HALLAM-BAKER

Okay. So I've been asked to talk about two different topics. I'm Phillip Hallam-Baker, principal scientist with Verisign. First I'm going to be talking about RFID. Then I will be talking about extended validation certificates. There is no connection between the two except that I am talking about them. (Laughter.)

So, first of all, what RFID isn't, or, rather, something that is often talked of as being RFID but really isn't, and that is you can take a smart card of the type that Neville is going to be discussing later with really strong security protections and you can add a wireless component and you can end up with a contact list. Smart card that some people will call a RFID card. What I'm going to be talking about is an EPC global RFID tag. The two are not the same. The contact-less smart card is to provide you security inexpensively at low cost. The RFID EPC global tag is designed to be negligible cost. We're talking about cents. Small number of cents. And they're designed to be produced in very, very large volume. We're talking about 100 billion a year. There are two manufacturing plants already set up to manufacture these tags at the rate of 100 billion a year. So that means that everybody in this room is expected to be having 20 of them a year. That's a lot.

So what are they for? They're all about supply chain automation. And here we have containers. Container ships are the reason why we have the quality of life we do today. If you look at the growth that we have in the western world, it's because of globalization, it's because you can now ship anything from anywhere to anywhere else on the planet cheaply and economically without having your ship tied up in port for days or weeks on end when you're unloading and loading it. The idea of this EPC global RFID tag is to enable a similar transformation of commerce by automating the supply chain at a deeper level further on down the line.

Now there's a problem here from my point of view as security advocate and that is that the security model of RFID tags is a security model of the bar code; i.e., anybody can read the bar code on your book or your product. There's no confidentiality there, and also, anybody can go to a photocopier and they can make you a bar code. Or, you can go to a site on the web and it will print you a bar code with any number you like. The other thing that happens is that once these things become really ubiquitous, and we're talking about the 10 trillion bar codes, sorry 10 trillion tags a year, and instead of them being attached to the pallet that the product is shipped out on, it is slapped on the product itself, such as a book. Well then you start to get a few privacy issues. Because as I'm carrying around my briefcase with 10 books in it, maybe those books don't change too much. First of all you can see that somebody is reading Das Capital and Adam Smith. You know, maybe you want to keep an eye out for that type of person. And maybe I am disclosing information about what I do, what I believe, what I say. But the other reason is that you start to have -- once it starts to be attached to clothes and so on, well you are going to know who somebody is just by the RFID tags that are giving out this spurious electronic junk to all and sundry without really thinking about it.

Now, there's another security problem that comes up, and that is: For applications today, one of the things that folk want to do with these is to tag pharmaceuticals. They want to control these pharmaceuticals fairly carefully because fake pharmaceuticals are a major problem. They are a loss of revenue problem and also there is often death. Think about fake chemotherapy drugs. It happens.

And so one of the big pushes behind RFID that Verisign and other companies have been involved in is how do you authenticate using the existing RFID tag? How do you lock down that

supply chain so you can't attempt to introduce fakes? It's a very challenging problem. Eventually you get to the idea of, well wouldn't it be nice if you could have that 5 cent tag have similar security capabilities to the $5 tag? Which means that you have to have a public key cryptography algorithm that you can describe in 20,000 gates or one slide. I'm not going to do it to you. I'm not going to give you an elliptic cryptography primer one slide. The technology is possible there, and if you're going to be thinking about schemes that involve people carrying around these RFID tags please, please talk to the technologists who are developing the next generation of RFID tags. We're not just the only folks who have a dog in this race but there are solutions. You don't need to be stuck with MIT's 10-year-old design now. There is another generation of technology. And you really need to be looking at it.

And just one final observation. You may know this guy. This is Victor Thurman. And he invented the first RFID tag. He did it under very specific circumstances. He invented it in Moscow after he had been kidnapped off the streets of New York by Stalin's secret police. And it was invented as an espionage tool.

So don't be ashamed of saying there are security and privacy implications. This is a technology that could be abused. What I'm saying here is that do allow us technologists a say and we can prevent some of those abuses. So on to my second point, which is extended validation certificates.

We have a problem with SSL certificates today. And some of you probably know about it. It's obvious. Not big enough for you? Well, that's the infamous padlock icon which appears in your browser. That's the only security information you get these days. That's the problem. It just isn't obvious enough. The other problem is that the user looks at that and thinks "it's safe for me to do e-commerce," and actually technically what it's saying is the communication between you and the server is encrypted. But are you talking to the right server? Are you talking to the bank you think you are?

And here is another problem in that when the SSL certificate was first introduced and Verisign introduced the first public SSL certificate, Verisign class 3, we were authenticating specifically the bank, the organization behind it. Since then there's a new type of certificate that's come along where they authenticate the ownership or rather holdership of the domain name. So instead of authenticating Busy Bank Incorporated, we're authenticating busybank.com. And there are legitimate reasons why you might want to have that. If you want to have a web cam in your house, you want to encrypt the communication between your browser and the web cam when you're looking to see what's going on in your house or maybe in the yard or whatever. You want encryption there. But you probably don't want to be authenticated to the same level of assurance that you'd want someone to authenticate your bank.

So these problems led a group called the CA Browser Forum to come into existence. And it's a group of CAs [certificate authorities], all the leading CAs, about 20 of them at this point and the major providers of browser clients. And they have been working on a set of criteria called extended validation. And at this point it is not an agreed standard. We're hoping to come to it. However, it is now deployed.

If you have the latest version of Internet Explorer 7, you get a new user experience if you go to a shop or a bank that has one of these new certificates. Instead of seeing the traditional white bar at the top of your screen, you'll see a green bar. So you have the address of the bar is now in green. Next to it there's a toggle that toggles between the name of the bank as authenticated by the certification authority and the name of the certification authority that issued that credential. And they're both important. I'll come to them in a moment.

The idea here is not about absolutely guaranteeing that there's no possibility of fraud. It's the executives of Enron company and certificates, and I checked that it's Enron, how can I stop them from having certificates? How can I tell that a corporation is absolutely definitely not crooked? But what I can do is determine if there's accountability. Is the location where I can go and serve legal process if there's a problem? Are they accountable as a matter of law? Are they accountable civilly, criminally? That makes a big difference because very few phishing criminals want that level of accountability. We want to know is the business accountable? But it's equally important, is the issuer of that certificate accountable? And that's the reason for that second display. I know that if I issue a faulty EV certificate, then when somebody is reporting that the phishing attack out here against a very well known bank, the picture will have my name, my brand next to it. So that's something that I'm going to take a great deal of pains to protect and something that my competitors are going to take a great deal to protect. So you've got accountability on both sides. The certificate holder. The certificate issuer.

Finally, just one thing about futures. We developed SSL class 3 certificates and there was 10 years between the first generation and the second. What I hope is that it's not going to take us another 10 years to get to the next generation in that when you authenticate the bank in physical space, you go to the ATM, it has the logo of the bank on it. You go to the branch, it has the logo of the bank on it. Every credit card they issue, every piece of paper that they send out, it all has the logo. And I believe that what we need to do is to take the Internet to that stage and have a means of securely authenticating the logos of the certificate holders and to display that in the browser in a secure way that cannot be impersonated by an attacker. And that's secure Internet letterhead which is my personal scheme that I've been working on for the past three years. So in a nutshell, extended validation is all about accountability, accountability for the businesses that are doing business on the Internet but also accountability for the certificate issuers. Thank you.

>>AVIVAH LITAN

Thank you.

>>NEVILLE PATTINSON

My turn to drive. There we go. Okay. So thank you very much, the FTC team for inviting me along this afternoon, I appreciate that very much. My name is Neville Pattinson. I work for Gemalto, we're the leaders of digital security. As much as we've come from the roots of smart card technology, we produce about 1 billion smart cards a year each with an operating system on it. First of all I have to give a disclaimer. I'm also a member of the Department of Homeland Security's data privacy and integrity advisory committee. And as such anything I say

this afternoon is my opinion and not the opinion of the committee. Okay. Disclaimer over.

So moving on, I've got the task to talk about smart cards and PKI. PKI after lunch is a pretty tough subject, hopefully we can make it a little bit interesting. But we'll start with smart cards. As has been mentioned, smart cards form a very important part of many of our lives today. Here's an example of an identity card. And, that little gold pad down on the bottom left, inside there is a chip, a silicon chip, fairly complex chip that's got everything it needs to do computations internally both as a CPU, a cryptographic co process, to help PKI operation. So any of you familiar with the Commodore 64 in your history? That's what's in here. That's what's in a smart card. That kind of power in one chip. But we have some more capabilities and they are getting stronger and faster every 18 months. But that's effectively the type of technology. A one-chip solution.

They appear all over our lives today. You might have seen them as DOD cat cards on the top left used for identification badges. You might have seen them now in your passports, electronic passports are now being issued. These are smart card technology. ID badges, Pay Pass from MasterCard is a smart card technology. Smart cards that you use to get around the D.C. metro, that's a smart card technology. We have a range of tokens that exist from our company and others that do one time passwords on tokens. Everybody who has a cell phone here today from one of the major GSM carriers such as T-Mobile, AT&T, you have a SIM card; that is a smart card in your phone. So these are very, very well-established in the world today.

Smart card technology is based on standards. They have been evolving for 25 years so it's about as long as I've been in the business. They are based on international standards through ISO. There are several of them. And as was mentioned by Philip the 14443 is the RF version of that technology. We have operating systems. One very common operating system is the Java card technology, which is now prevalent on many of the smart cards produced in the world today.

There are life cycle management tools such as the global platform technology, which is added to the operating system to manage the card during its life. Then, we have specific applications. Sorry for the typo there, I missed an L. Application specifications -- you have the paper. You have EMV for chip and PIN as it's sometimes called for financial transactions. For the HSPD-12, the directive in August 2004, the 5201 specification now exists for identification credentials for all government employees and their contractors. We also have from the international civil aviation organization machinery little travel documents for electronic passports.

Take a look at a potential smart card. I've taken the levity to take the chairman's picture here and look at what could be the PIV card that's probably not quite to the specifications. I apologize for that, [indecipherable]. I can see him sitting in the audience here. So this is a smart identification card. You can have an RF antenna inside the card body. You don't necessarily see that. Many of you have probably used them to get into your offices. You touch them on the door to get in. You have a photo there for visual verification of the flash pass. You have the smart card chip that can be used at the door or at your computer to log in. And you have various security features, printing and holograms and so on, on the cards themselves to help authenticate

the card visually.

Smart card security is all about trust. It doesn't trust; this little chip doesn't trust anything until it proves what's going on in the world about it. It needs to know that there's somebody here that should be using it. It needs to know that it's communicating to a terminal that it should be allowed to talk to. This physical security is in the silicon. The way it's designed, the silicon vendors spend a lot of time creating all sorts of sensors and counter measures at the silicon level to start people probing and taking them apart. We have hardware security mechanisms. Tamper detectors and scrambling of buffers on the CPU. We have card package security mechanisms where you can't peel them apart or dissolve them and get back at the chips.

Operating system. As I mentioned this is the strength of our own company where we create operating systems that run these smart cards intelligently, and we've got lots of tampering detectors in there. Logical security measures for encryption, digital signatures and so on and we have application security that goes on as the final layer. So smart cards are very well-established and have proven their ability to operate in high security applications.

I think you've already mentioned and heard about RFID. I'll just reiterate. This is not RFID smart cards. RFID is a unique type of technology as has been discussed, and I won't dwell here. It's much cheaper and it's much more simple. It transmits the serial number in general and the newer ones are transmitting a little bit more than a serial number. Generally, that's its job. It's to be identified and to be tracked. This is not the technology of smart cards. Smart cards are sophisticated microprocessors as I discussed. But they are capable of preserving the privacy of the information they hold and preventing it against skimming and eavesdropping and duplication et cetera. They are privacy enhancing. They are identity verification devices and can be used for that purpose for human identity verification. RFID is not that technology even though for some reason DHS has decided to use it for the proposed pass cards for crossing into the Canadian and back into the United States. An RFID will be used in that respect for tracking humans. It should be reconsidered. 4,000 comments were issued to that NPRM of which only three were in support of that system, 3997 opposing it. DHS apparently still is proposing to use RFID for that.

Looking at the relative positioning. Bottom left, you have animal tagging, inventory tracking, which is where the low cost, high volume RFID technology is in its element as it's been discussed by Phillip earlier. To the top right where we're trying to protect information, identity and so on, we have several different types of smart cards. Not just one but three types: the transit tickets, the payment cards, and government ID and corporate IDs, and electronic passports for that matter.

So smart cards, there are many varieties of them. Contact-based and contact-less. They are RF-capable. They are small, secure, powerful, portable computers. Open standards. And many companies can compete and supply these to the government and to corporations and to businesses. They have been evolving for 25 years and continue to do so. Moore's law every 18 months or so they double in CPU power, double in memory and get even more clever at defending themselves against attacks. They are proven and cost-effective. They are widely used in U.S. government programs today for identification purposes. The DOD cat card passports and

transportation worker identification credentials 5201 registered traveler, first responders, these are all in place today and many of you have probably seen these or used them.

Let's move on to the second subject. Public infrastructure. The easiest way…I'll let you read this. The easiest way to describe this is PKI is a way of life digitally. Verisign are one of the key providers in this area of certificates, which I'll discuss shortly. PKI is about trust. How do we dis-establish between one person and one other entity? How do we form trust? And that is by having certificates which are a digital representation of how we're going to validate and authenticate each other.

So PKI infrastructure is a closed system of certificate-based credential management. Everybody has a certificate. Everybody is going to have keys associated with that. You have physical security for buildings that you might be able to use within your PKI. Logical security to log into your desktop to secure your email by digitally signing your email and doing encryption by key exchange using digital certificate technology. Secure websites through SSL that you're familiar with the little lock that was described and further on for the extended authentication that we now see. Remote access through VPN and dial-in are all part of certificate-based technologies to allow you to authenticate yourself securely to those services. File encryption and so on. And we don't need certificate authorities to manage these trust chains of these certificates to work back who we can trust and where we're going to get them from.

Identity management systems are incredibly important to PKI. You need to know who you have in your system and who they are therefore going to be trusted to communicate with. Obviously, if you involve cards, there will need to be a card management system to support that, too. The certificate is a question of trust. How do I trust the credentials of the other party? Well a certificate is your public key of a key pad. For PKI folks, you have a one time generation of two pieces of information, a public key and a private key. Two mathematical related keys. One key you keep secret; the other key you keep public. And by making a certificate out of the public key, you can allow people to communicate with you and you can communicate with them with a deal of trust.

Certificate authorities are used to create the certificates to then provide them and to the public key infrastructure. You have to publish a public key and a certificate in order for people to be able to receive it and to validate your communication with them. There are standards involved on certificates. The X509 standard is the core of that. Certification authorities are those entities that are presenting themselves to provide that root of trust. How does an enterprise, for example, get their own root certificate? They go to a certificate authority. They get issued that and then they start to create certificates with their own certificate of authority and so on.

There is a tree of trust that comes from fixed points within the infrastructure. So common PKI cryptographic services provided by a combination of smart cards and PKI, authentication i.e. establishing trust. How do I know who am I dealing with right now? Can I trust them? What is the purpose of the communication? Is it valid? Is it authentic? You can do that with PKI and with certificates. You can perform bulk encryption for disks and so on communication. Digital signatures, as I said, for signing and verifying the integrity on

authentication of the individual who is the sender. You can do secure email through SMIME for confidentiality and integrity and you can do secure web access. These are all services that PKI provides and can be supported by smart cards if you so choose.

So smart cards, I see them as like a little security agent of the issuer in the hands of the user. Like a little security agent that everybody has. Smart cards can verify the user and authenticate the system creating a chain of trust. Smart cards provide portability of that credential. You take it with you. It is not left on a hard drive. It is in your pocket when you want it to be in your pocket. In the computer when you want it to be in the computer. You can use the PKI service for non-repudiation to make sure that you can prove who you say is doing the transaction. So smart cards are proven cost-effective, tamper resistant counter measure to identity theft. Thank you very much.

>>AVIVAH LITAN

Thank you.

>>MARC GAFFAN

Okay. So I will reintroduce myself. It's been a long afternoon. I'm Marc Gaffan. I'm with RSA, the security division of EMC. Quick poll of the audience, who knows what or thinks they know what risk-based authentication is? Not a whole bunch of people. And one of the reasons is it's a pretty new. I may even call it "technology," a concept for supporting technology. It's in use today by more than 100 million users, probably most of you as a result of last year's FFIEC guidance for online banking. And I'll dive in and explain a little bit more about what risk-based authentication is. The concept or the framework is essentially to always consider the risks during authentication. Authentication used to be, or was traditionally thought of, as something as binary. You've either managed to authenticate yourself or not. If you've authenticated yourself, you're free to do whatever you were deemed to or whatever the credential enabled you to do.

We're now talking about not considering a credential in a binary manner. We're talking about using a credential or considering a credential in the light of the risk that this credential is used within. Okay. We're looking to strike between, strike the balance between usability and security so we can help specifically consumers with the most security but provide the best possible user experience. Essentially enabling just in time or just strong enough authentication. It means using incremental levels of authentication dynamically based on the risk at a given time calculated in realtime and based on a policy to decide what level of trust to grant to that authentication method and basically decide to let the user do what they're trying to do. Or, if further authentication is required because we think that they're doing something that's riskier than usual, require something stronger than that. Obviously configurable by the type of your organization, what their policy is, what type of consumer base or what type of authentication base they have. And all done in real time.

The essence is essentially to let users transact in the way they've been used to transacting before. The baseline could be very different based on the application. Take an online banking

institution, for example, up 'til recently, most online banking applications let you log in with a user name and a password. The notion here is to keep users logging in to their online banking using a user name and a password. When they do that, behind the scenes goes through a very, very rigorous risk analysis that's transparent to the user and make a real time decision based on the risks, based on the analytics and based on the institution's policy about what to do next. If the policy and the risk yields a high risk situation, it will trigger additional authentication in various forms depending on what that customer base is used to using, what are the economics of deploying an authentication technology. What's the risk that this specific transaction, this specific individual has got or now pertains? And based on that decide what, what we call secondary authentication, lever to pull. But in most cases, because most of us are genuine users doing the genuine transactions, let users log in when it's low risk in an un-interfered manner. Let them do their own thing.

Obviously, the business drivers behind this are the less you inconvenience customers, the more of an adoption to the channel there will be. So things that are easy to use, people will use more. It's also much cheaper to deal with authenticating or to changing the user experience for one, two or three percent of the population, only the high risk rather than the entire customer base and having to deal with customer service issues, exception handling, et cetera. Essentially trying to balance between the risk level, the customer segment whether it's a business banking or consumer banking customer, and the institution's policy.

What you need to support that is strong risk analytics to be able to determine what's risky and what's not, and also wide portfolio of secondary authentication methods for those exception handling events. What do you pull out of your hat when you need to apply stronger authentication when you think this is a risky situation. So what we're talking about is a paradigm of having all of these multiple types of authenticators. Each institution, each company can have their own methods of authenticating or strong authentication methods to authenticate their customers, but applying them in a risk-based fashion based on risk, based on risk analytics and based on a policy and also based on shared information. What do we know as a community collectively that pertains, that can contribute to the risk of this specific individual? And I'll talk about that in a minute.

Specifically when we're talking about consumer applications, and this is an example, this is the example of the framework implemented in a consumer environment. Remember this is a framework. You can take this and decide to apply this with the usage of one time password tokens, biometrics, et cetera. This is just the framework. The way this is being implemented very, very widely in the U.S. is to look at the following risk indicators or the following pieces of information to establish the risk of this specific transaction. Looking at things like the device, can we recognize the device? And attempting to do this in a passive manner. So when I log into my bank website, they can recognize if this device is interacting within my account. So I have previously used this specific device multiple times in the past 90, 120 days. If that's the case, most likely it's me. Look at circumstantial evidence on the device. So, not only a unique device identifier, which can be sometimes removed from that device, but look at the circumstantial evidence on the device. What type of characteristics do we have? Looking at all those parameters transmitted today, somewhat standard HTTP transmission, some are extended characteristics of those devices and try to make an assumption of regardless of whether that's got

that unique device ID or not, is that still my device?

Another thing I'm looking at is a networking infrastructure of sharing information among institutions. Today there's a network in place that shares real time information of fraudulent activity such as IP addresses and device IDs that have been used previously to commit fraud. If you have insight to that type of intelligence, you can make smarter decisions on when to authenticate people.

Think about if we had no Secret Service, if we had no underlying intelligence, what type of screening we'd have to go through to get into buildings, to get through airports. The reason we can go through acceptable processes is because there are underlying technologies to do that. This is the same type of concept. The other thing is looking at what that user is doing. If I'm logging at the first of the month, I'm checking my balance, I've been doing that for the past two years because that's when I get my paycheck and I want to make sure I have got money in my account. That's a low risk transaction. And that's probably me doing that just the way I've done it, as I said, for the last 12 months. But if someone logs into my account today from an IP address that's in Nigeria -- and nothing against Nigeria, I've just never visited there, ever -- it's not the first of the month and someone is doing a high risk money transfer to an account that I've never transferred money to, that's something that's high risk. Now obviously these are two different extremes. You don't need really sophisticated risk analytics to be able to distinguish that that's low risk and that's high risk. But even someone logging into my account from an IP address that's an address I never logged in before, maybe that individual is trying to collect information about me through that account and will maybe use that information on another channel, like the phone channel. But the area, the compromised area was initiated on a web channel, with a low risk transaction, in fact no monetary transaction at all but just exposure to personal information that can then be used for further verification.

Looking at what the user is doing within that session, okay, so not only looking at specific activities but looking at the sequence of activities. Someone opens up a new account destination or payee and goes immediately and transfers money there, that's something you should look at. If someone logs into their web session, changes their mailing address, calls up a call center, resets their ATM card and then asks them to send them a new one, you need to know that sequence of events to be able to correlate that there's a potential fraud attempt here and triggers stronger authentication as a result of this insight, this risk analytics. So obviously got to be self-learning because our behavior patterns change. Specifically on the web, which is a new emerging technology. Some people are getting onto the website or starting to bank online for the first time. Systems need to be tuned enough or smart enough to realize that this is an emerging channel, essentially, and be able to identify anomalies within that context. So that's the context or that's the framework of risk-based authentication.

>>AVIVAH LITAN

Thank you. And our last speaker.

>>MICHELINE CASEY

Good afternoon. I'm Micheline Casey, senior director of identity management for ChoicePoint government services, and I appreciate everybody coming back after that beautiful lunchtime hour and a half that we had. I'm going to be focusing on knowledge based authentication.

But before I begin, I wanted to give everybody a brief overview about who ChoicePoint is in case there are some people here who are not familiar with ChoicePoint. As an organization, we're a billion dollar revenue company, spun off from Equifax in 1997. We are publicly traded and have been since we spun off 10 years ago. We provide data analytics and information solutions to our clients, both commercial and government agencies to help them manage both physical and economic risks. And since our data breach in 2005, we've implemented numerous policies and procedures that have become a model in the industry. I think we're a bit unique relative to the other technology people that are on the panel today in that we're the only company on the panel that are solely focused or has a particular focus within our company on identity proofing.

I'll apologize in advance to Avivah. We use slightly different terms than she did. We use authentication where she uses identity proofing, and we use authorization where she uses authentication. So you will see a difference in the terminology that I have in my presentation. I'll try to stick with her terminology. So what we're trying to address over the course of today and tomorrow is really getting to the key question of: Are you who you claim to be? Am I really Micheline? Is this really Avivah? And we've heard a lot this morning about the problems about identity theft, hacking, phishing efforts, pharming, and we also heard on the real ID panel some of the problems with the breeder documents and the circular references that exist between the birth certificates, passports, drivers' licenses, et cetera, as well as the ease with which one can create a false birth certificate or in the case of the 19-year-old, a false driver's license. So I think we're at a point now in society where unfortunately there is a real risk of accepting a false or assumed identity based on just those pieces of information whether it's biographic data, a breeder document or financial account information. So the key question is, then, what is the solution that we can use to help proof an identity? And just because I show up with Avivah's driver's license and maybe her financial account information, does that mean that you as a business should let me open an account, apply for government benefits or purchase a flat screen TV?

Again getting to the core of the questions, how do you truly proof or authenticate that someone is who they are claiming to be? Knowledge-based authentication, which is what I'm here to talk about today, is an extremely effective technology to doing this. KBA, or knowledge-based authentication, takes place in two primary steps. The first is vetting or verifying that an identity does exist. Is there really an identity called Micheline Casey? And the way that we do that is by taking the presented identity attributes, name, date of birth, Social Security number and perhaps address and looking for anomalies in that data or risk or fraud indicators in that data. Perhaps a Social Security number was issued before the date of birth that was presented. Perhaps that person has five Social Security numbers that's associated with their name, et cetera. That would be an indicator for fraud.

Once we've actually verified that an identity does truly exist then we authenticate that

individual. Is this person claiming to be Micheline really Micheline Casey? And how we do that is through a generation of what's called a smart quiz. The smart quiz typically can be anywhere from 3 to 7 questions based on historical data about that person's identity. Those questions are culled from a combination of public record sources, proprietary data sources and private data sources that perhaps our customer or the government agency owns. The level of authentication is dependent on the risks associated with that particular application. And so the smart quizzes themselves are extremely customizable depending on what the client's needs are and again the level of fraud and also the demographic base of their typical target population.

Once we've authenticated that the person who is claiming that identity truly does own it, then the client can go ahead and grant the authorizations, the rights, the privileges, et cetera, that the person is trying to get. The next thing about knowledge-based authentication is it's an extremely flexible and complementary technology to any of the other technology that the other panelists have talked about today and some of the others that haven't been mentioned, but where our primary focus is again on that upfront identity authentication piece. It is the most critical piece in an enrollment process or credentialing initiative.

As I said, it can be used in conjunction with issuing a smart card or with biometrics or in conjunction with PKI. Again, it's that upfront identity bending piece and is a great part of a multi-factor authentication strategy. Just to quickly close, again, we understand, we've heard the issues today and accepting just personally identifiable information or breeder documents and the risk that it leaves agencies and organizations open to. Knowledge-based authentication and utilizing the smart quiz to authenticate someone's historical information that only that individual would know is a very effective means of preventing fraud and reducing your risk as a business or as an agency. It can be used with both physical and logical access. It can be used as a stand-alone technology or in conjunction with multiple other technologies and it can be used across multiple customer channels. Whether you're dealing with someone over the Internet, whether someone is standing in front of you in a retail situation or someone is coming in through a call center or IBR process.

Again the enrollment piece, that up front identity vetting piece, is the most critical piece of any credentialing process. Particularly if you're dealing with biometrics because once you've linked a biometric to an identity it becomes extremely hard to de-link that information. And really the vetting is the most critical piece of the identity architecture. As a commercially acceptable best practice that's been recognized by multiple industry groups and has been utilized quite highly in the commercial space as well as government agencies, what we've experienced is a high rate of customer acceptance and a good customer experience, which we talked about this morning that was very important. And in our experience, consumers are willing to take that extra step to vet themselves if they understand that a business or an agency really is seeking to protect their identity, their privacy and their information. Thank you.

>>AVIVAH LITAN

Thank you. My goal in the next few minutes is to summarize what you've heard. There's like a whole range of technologies. If you're like me, you're just trying to sort it all out. Because if it was really as easy as everyone says, we wouldn't have any problems like we have

today. So we are making progress, but these technologies are much easier said than done. And there's still a lot of implementation issues. So I'm going to ask the panelists to summarize the strengths of their technology in one minute, 60 seconds. You maybe could even go to 90 if you really need it. And then we're going to go through the challenges of the technologies. So we'll spend a minute each on the strengths. Just summarize what your technology does and why it's the best or why you promote it. And in your case, Phillip, I would talk about extended validation certificates as opposed to RFID, but it's your choice. And also understand that Marc's not really talking about a specific technology. He's talking about risk-based authentication. So they didn't really have time to prepare for the 60-seconds piece. But that's one thing I learned in business school, not that I went that long, but if you can't tell your value proposition in the elevator, then you don't really have a good clear value proposition.

>>VICTOR LEE

No high-rise elevator pitches, I suppose.

>>AVIVAH LITAN

We'll start with you, and we'll go down the line Victor; just give us a 60 second value proposition why biometrics is something you advocate.

>>VICTOR LEE

Biometrics complements, as I said before, what you have and what you already know by adding the component of what you are. That's very critical because it adds something that we haven't been able to utilize to leverage in the past. Something that's very personal about us, that's hard to transfer, hard to duplicate, hard to fake. And as a result of that, it helps increase the level of security that we can have or at least the level of confidence that we have that a particular individual is who they claim to be. It's not a perfect solution. There are still a lot of ways in which you have to be very careful about the particular context in which you're deploying the technologies, but it's definitely a facilitator, it's something that should be looked into with great care and with great ambition in how it can be deployed effectively.

>>AVIVAH LITAN

Phillip?

>>PHILLIP HALLAM-BAKER

Since I sell every product which is on this panel, I'm not going to be saying that one is best. However, think about the problems that we have here, phishing is credential theft by impersonating a trusted party. So one part of the solution is certainly better credentials that are harder to steal, harder to fake. But if we don't also address the problem of how can you be sure that it's your bank? Then that new generation of credentials isn't going to provide you with real value. There will be a new set of attacks. If people can impersonate banks and other trusted parties on the Internet, you're always going to have problems and extended validation is the

platform to set that right. It's got to be a component of any sensible solution here.

>>AVIVAH LITAN

Thanks. Neville?

>>NEVILLE PATTINSON

So I'll talk about smart cards rather than PKI, I think I got smart cards off pretty well here. Smart cards are proven, first of all. I suspect most of you sitting in this room probably have one if not two on you in some form somewhere. They're widely adopted. They're very cost-effective. I'm only talking a few dollars not cents as RFID tags. A few dollars. We're not talking about tens or hundreds. They're very, very good and proven to protect citizens' privacy from electronic passports which all of the American citizens here will be getting soon, you will have your credentials protected in your electronic passport through the technology of smart cards. They will work in conjunction with PKI and biometrics. We can match the biometrics inside the chips or off the chips, whatever is needed. It can provide that strong authentication of the user is who we say they are. And we can be greatly confident that this is the person we want to transact with. And on that basis, I think smart cards perform a tremendous foundation for protecting against identity theft.

>>AVIVAH LITAN

Marc?

>>MARC GAFFAN

I, too, will not say why risk-based authentication is the best technology out there but rather what it's good for and what it's not good for. I think there are three main things that risk-based authentication is good for is: (A) balancing between security and usability, making sure you've got the right credential at the right time with the right level of strength. That's the framework. Insuring you've got a flexible framework so that when a specific technology, authentication technology becomes obsolete because of the fact that it's been hacked, you don't have to rip out your entire back end system or your policies et cetera.

You can insert something that's extra. You can step up to that authentication technology or that the new generation technology when it's required and only when it's required, not across-the-board in a costly fashion.

The third thing is it's future proof. It's future proof because of what I mentioned in my second topic. It's a framework that as things become obsolete, you retire authentication mechanisms, you enhance your risk analytics to address new threats, identify to new threats, and then you implement stronger authentication methods that can address those threats when they are detected.

>>AVIVAH LITAN

Thank you. And Micheline?

>>MICHELINE CASEY

I'll address authentication. Strengths of KBA and identity proofing, again going back to -- going beyond the acceptance of breeder documents or sensitive personally identifiable information. Secondly, it is device diagnostic. It can work in conjunction with any of the technologies that are up here. There's limited vulnerability to hacking or phishing. The questions that are asked are pooled from an extremely deep pool, wide and deep pool of information going back up to 20 years and for multiple, multiple data sources. So, it becomes extremely hard to guess which questions are going to be asked each time you come back or which series of answers are going to appear. Additionally, you don't have to have multiple smart cards or other authenticating devices that you would have to carry around with you.

>>AVIVAH LITAN

Okay, thanks. So that's a summary of the benefits. I'm going to play devil's advocate and ask each of you about one weakness that I perceive in your different technologies. But first let me just see if you have any questions in the audience or if any come up? Yes, sir.

>>AUDIENCE MEMBER

One question that I would have or one thing that pops to mind with a lot of the technologies you presented is the privacy issue and data protection issue because I look at for instance biometrics or the knowledge base authentication and to a certain extent also risk-based authentication you will be storing additional attributes about your user base in order to be able to actually authenticate them. So that additional information, like for instance the data going back 20 years, or additional biometric information is exposed in some sort of an attack, you will probably be liable, to a certain extent be liable, for that additional information being dispersed. So I would like to get your comment on how to address those things.

>>MICHELINE CASEY

With regards to knowledge-based authentication I think we're talking about two issues, privacy and security. With regards to the privacy aspect of it, we make sure that no information is actually returned to the customer or to the consumer as part of that quiz process. We pass flags back or identity scores back. The other thing is we don't allow the clients to know which questions the consumer actually got wrong, which helps to alleviate insider identity theft. Secondly, there is no kind of great database in the sky with all these questions or with all the answers. So it becomes extremely -- if you're talking about hacking, there's no single, central repository to hack into. Harvesting becomes extremely difficult.

And with regards to the security of our data and our systems, we're audited annually as part of a SAS70 audit. Our data centers require biometric access actually to get into those data centers and since our data breach in 2005, we've had over 40 or 50, I'm sure my senior

government affairs person back there could answer that better, independent audits from government agencies and commercial entities, and we've passed every one with flying colors.

>>AVIVAH LITAN

You're speaking about ChoicePoint. I just want to bring up that there are other data brokers that are not getting audited 50 times a year and there's no regulation on them. Yes, sir?

>> AUDIENCE MEMBER

Antiquated nature of –

>>AVIVAH LITAN

We can't hear you.

>> AUDIENCE MEMBER

Given the antiquated nature of a SAS 70 evaluation, and audits traditionally being only checklists, when was the last time you underwent a penetration test?

>>MICHELINE CASEY

We do those annually as well with an independent auditor, independent outside auditor.

>>AVIVAH LITAN

Actually they're not the best example because they actually have really good security and privacy now that they're being audited. I know that you would have had it even without the audit. But I am just really surprised, as a fraud manager from a major bank showed me what's available on me for $25 on the Internet at someplace called Locate America. And there are a lot of those out there. And they haven't undergone any penetration tests. The data is kind of a big database in the sky. And I think it is something everyone has to worry about. Is there another question in the audience? Yes, sir. Then we'll get to the others.

>> AUDIENCE MEMBER

My name is Richard Bartell (ph); I'm an officer in the financial crimes unit of the D.C. metropolitan police. I had a question about how you brainstorm the perspective of the criminal. In other words, there are many criminal organizations operating out there who have very high profit margins. And they look at these strategies and look at the way that these defense mechanisms are structured. Do you, in your organization, brainstorm and create teams of people that would try to think like who's going to break in and how? And provide guidance to your customers in that area? And I bring that to the fore because there was a lead article in USA Today, today on the front page about cyber spies exploiting various software features to get themselves like a Trojan horse into an authenticated system.

>>AVIVAH LITAN

So let's start with Phillip and then Marc.

>>PHILLIP HALLAM-BAKER

There's something called I defense which provides a very comprehensive intelligence service on electronic threats, Internet threats across a broad range. They use a large number of techniques to monitor those threats, including the obvious ones of observing public sources such as what viruses are in the wild, but also going into the chat rooms and other techniques. It's a very comprehensive service. Working out -- actually there's one thing I'd like to put to rest here and that is the silly notion that it takes a thief to catch a thief. It doesn't. The best way to catch them is to get a bunch of thieves together and bug the room. (Laughter.)

>>AVIVAH LITAN

Good point. Marc, do you want to follow-up?

>>MARC GAFFAN

Similar to Verisign, at RSA, we have what we've called the antifraud command center which is a command center that monitors those underground chats and correlates that with some of the information that we come up with from other various products. These include our phishing products and our online banking prediction products putting them together and looking at the vectors of attacks that are starting to happen across channel now as well is something that, that's the methodology that we use in order to try and stay ahead of what those fraudsters are doing.

>>VICTOR LEE

I'd say from a biometric standpoint, it's always going to be a game of cat and mouse. Insofar as people with resources are always going to find ways to break into the systems. Instead of necessarily trying to figure out always how you can defeat them, you can either try first to anticipate what the techniques are going to be that they use. One of the efforts that IBG, for example, is doing is we're doing a spoof effort where we're intentionally trying to trick some of these devices and figure out what their vulnerabilities are in advance, before they actually are deployed to widespread without careful consideration for these potential problems or limitations.

That doesn't mean to say, though, that just because the technology has a particular weakness, it's therefore inapplicable to certain scenarios. One good example I've used is a hand geometry technology which is developed by a subdivision of Ingersoll-Rand, the large construction company. Their concept is it's a hand geometry device that essentially takes a 3-D picture of your hand for all intensive purposes. It's not that difficult, theoretically, to create a model of a hand and try to trick a system. But, if you're deploying it mostly for time-intensive functions, to stop a construction worker from buddy punching from their friend, that particular context in which it is deployed is probably okay. Not many construction workers are going to

take the effort of going ahead and making a model of their friend's hand just so they can get an extra 5 bucks on whatever minimum wage is today, 7.32 whatever the case may be an hour. It's not worth their time and worth their effort. So it's a reflection also of the context in which the technology is going to operate.

And then I guess the other final point I want to bring up is that in many ways, again, I hesitate to say any technology is perfect, but the question is how can we create as many deterrents as possible? And, look, essentially people who are trying to penetrate a system are going to look for the weakest point. The idea is if you can create more and more road blocks so that that weakest point is hard to get to, whether it's using multiple levels of technology, multiple combinations of technology that might facilitate the ability for a deployer to have a robust system without being too afraid of the vulnerabilities inherent.

>>AVIVAH LITAN

Any other questions before I ask one? So I'm going to take a practical example of what happened at TJX and look at how your technologies or technologies that you're talking about could have stopped that. And that'll make us look across channels because here was a case where I don't know exactly what happened but data was sitting on some server that no one was really paying attention to. And they were able to take this data over the course of a couple of years and then go use it because there was no strong authentication on those cards. There are in Europe, but EMV hasn't really worked in solving fraud; it's just worked in migrating fraud.

So let's talk about a practical example and ask the question: What types of fraud can these authentication technologies stop? And what percentage has actually been lowered because of user authentication technology? So go back to the practical example. There are hackers out there that are going back to the gentleman's question from the police department. Who knows where these guys are going next? You may have all kinds of intelligence. You're following their chat rooms so that they can just show up least expected spots. How's biometrics going to work there? How is mutual authentication and site authentication going to work? How is risk-based authentication going to work unless it's deployed everywhere? How will smart cards work when you don't have cross country use of that? When banks in the United States don't want to spend money on it. How is knowledge-based authentication going to help if someone is going to a store and buying something at Wal-Mart? Sorry to put you on the spot, but let's be practical about -- I think you said it, Victor. You can't solve everyone's problems. You have to raise the bar. But how would biometrics play out in that situation in a TJX breach?

>>VICTOR LEE

Well, one of the ways in which biometrics can be utilized is both for the logical access control and also the physical access components of it. To be able to, as I said I like to think about the context in which these systems are operating. And also part of the challenge if I can step back for a moment is to think about how interoperable some of these systems are going to be.

One of the challenges that say biometrics is facing is that a lot of these systems which

might work perfectly fine within their limited environments may not be able to work well with multiple other systems that exist across the nation. That could be a good thing. That might mean that a breach is going to be limited to one particular area, but it also can be a problem in so far as systems never really learn from the mistakes that perhaps other systems have encountered. In and of themselves, the biometrics have the ability to make it more difficult for a person to break into a system and to be able to do much once they have broken into it. The challenge is going to be, as somebody said before, that if somebody is successful in breaking into a system, how do you go about actually changing your biometric.

As a gentleman had mentioned earlier today, there is a concept of say cancelable biometrics, where before you actually create that new template from an image of a biometric that's captured, you do a little distortion on it so that it gets compromised. No problem we change the encryption method and you get a new sort of pseudo biometric. The problem with that is somebody comes out with a fake finger again. They're just going to go ahead and reauthenticate themselves and they're just going to create the new re encryption. You're in the same problem, the same hole you were in before.

>>AVIVAH LITAN

Basically, you're saying it would limit access on the systems where you implemented it.

>>VICTOR LEE

Both logically and physically, yeah.

>>AVIVAH LITAN

How about you, Phillip, do you want to add to that?

>>PHILLIP HALLAM-BAKER

Well I told the wife not to shop at TJ Maxx anymore, after all her credit cards had to be reissued.

Well firstly they were going into a legitimate authentic TJ Maxx. So obviously EV is not an issue there. However, there is an accountability issue. Can I mention my book?

>>AVIVAH LITAN

Sure.

>>PHILLIP HALLAM-BAKER

In my book on Internet crime which should be coming out in the fall, I identify accountability as the key deficit behind almost every Internet crime. Here the accountability issue was why on earth were you storing all that data in the first place?

In the credit card rules, tell you that if you divulge that information, you are fined 50 bucks per card that you've divulged because the bank that issued that card now has to reissue it and there's cost there. So the merchant that disclosed the data is charged for the cost that they've incurred. And so there is accountability in the system, which I would guess is about to hit somebody in that company. You shouldn't have had that data unencrypted on your disks. As soon as you took the data at the tills, it should have been encrypted and the decryption keys should have been held offline if you needed to keep the data at all.

>>AVIVAH LITAN

Good point. Neville?

>>NEVILLE PATTINSON

I think a little bit can be augmented onto what Victor was saying about biometrics, about physical and logical access. Smart cards can provide that linkage between the human and the biometric, the system. I'd like to think of it as a trust triangle that we're looking at here. The triangle being on one point the issuer who has given you the credential and issued you the smart card for you to bear as the user. So the user's on the second point of the triangle, and the person who's receiving it or the server or whatever is the third part of the triangle. So we're trying to create trust in that triangle that the issuer is authentic, that the card is authentic. That the relationship between the card and the user can be proven.

So we know who should be bearing this card, that the card is good and that it can now be accepted and trusted by the receiver. So without this, you're left with biometrics or you're just left with other things. The card provides that little computer to do that authentication. It can verify the user's present by biometric or by PIN. It can then verify to the servers, or the receivers, or the issuer as well to prove that it's authentic. On this basis you get the chain of trust and essentially the trust triangle between these three elements. So by having this, accessible information is protected, by having to physically use these, by physically having to authenticate to them, and for them to have to validate to the equipment. So you create lots of steps and checks and balances of authentication before you can get at information. If you don't protect it with technology such as biometrics and smart cards and PKI, it's not protected sufficiently in my view.

>>AVIVAH LITAN

I just want to stop on Neville because I would agree that if the U.S. banks had smart cards, it wouldn't matter if they stole data. It wouldn't work at the point of sale.

So given that, why is there so much reluctance to upgrade to smart cards in the U.S.?

>>NEVILLE PATTINSON

I wish I knew the answer to that. That seems blatantly obvious to me they should.

>>AVIVAH LITAN

As a practical matter, what do you think?

>>NEVILLE PATTINSON

There is an issue of infrastructure. The infrastructure historically is a magnetic stripe and there's a huge in-store base. Essentially in the United States, local calls and Internet and so on are much more prevalent than in other countries. Therefore online authentication of transactions can be done free and easy. In other countries, in Europe, local calls aren't free, et cetera. It costs money to make a phone call. So by avoiding having to make a phone call to authenticate a transaction, if they can do it with smart card, it can be done off line. It's a managing risk again. Can we be certain that this is an authentic card? Yeah. Is the right person using it? Not really sure but it's got a smart card and they PINed it so probably pretty good. They can therefore not have to do the online verification. The U.S. doesn't have the same business model; they don't have that price.

>>AVIVAH LITAN

It's a cost issue and the fraud just hasn't been that high.

>>NEVILLE PATTINSON

The issue is that in Europe, you generally have four or five banks per country. And every bank that is an issuer is also a merchant acquirer. And the two businesses roughly speaking balance out at every bank. In the U.S., you have 10,000 banks issuing the cards, give or take a few. However, the merchant acquirer business is concentrated much more tightly within I think it's something like 10 acquirers of the vast bulk of the business.

>> AUDIENCE MEMBER

25 billion merchants run by Visa. I'm in that bank. We're the ones who suffer. When that card is compromised, they don't pay a dime. That infrastructure, that decide to swipe the card… They don't want to pay for it.

>>AVIVAH LITAN

I'll just repeat what you said. I think I can paraphrase it. You're representing retailers?

>> AUDIENCE MEMBER

No, I'm with the credit –

>>AVIVAH LITAN

Do we have a microphone? We want to hear what you're said because you're sparking a good debate.

>> AUDIENCE MEMBER

The problem is that the costs and the benefits are not precisely aligned here. And in Europe it didn't matter too much because the costs and the benefits were two businesses within the banks. And they could be told by the top floor that they were going to deal. You don't have a top floor in the U.S. telling them to deal.

And to be more specific, when you have Visa, you're dealing with 25 million merchants. And, true, there is the connection to the banks just as you described. We're down to 10,000 including banks and credit unions. And everybody is getting some fees on this. But 25 million votes carries a lot more weight when you're talking about who's going to pay for that reader? That new reader for the chip. Because we know we're the last country. Mexico is even going into the chip. Canada. It's all around us. But who wants to pay? Why don't you guys pay, meaning the issuers? Meaning banks and credit unions? Why don't you pay some part of it, because it's in your shop? It's an argument. And I'm afraid that's where we're at. I see no -- exactly what you said, we can deal with 2% fraud except for us. We don't just have TJ Maxx. BJ's from 10 years ago compromised it. We still have yet to get them into court.

>>AVIVAH LITAN

Good point. And I hear that the estimates for upgrading to smart card infrastructure, what are they? What are they 30 billion or more? And who's going to pay for it? Right. The cost of fraud's lower than the infrastructure. Give him back the microphone.

>>AUDIENCE MEMBER

28 percent, cuz I've had argument with them. 28 percent return on equity. That's pretty good. Well my argument was to say, "Gee, you're losing 2 to 3 percent. Wouldn't you like to make 31? No. The costs, we'll deal with it. We'll stick with our 28." Pretty hard to argue economics.

>>AVIVAH LITAN

Right. That's the fundamental issue. Who is going to pay for all this great technology.

>>VICTOR LEE

Financial services are pretty slow adopters, I would say in general, of technology. That's another factor coming into play. If we see government [?] that are already using smart cards and other related technology in an effective manner, then perhaps the financial services industry will become more willing to jump on board and go ahead and take that.

>>PHILLIP HALLAM-BAKER

The other thing that comes up in these discussions is that when there have been attempts to have that type of discussion, they have a habit of being canceled at the last minute in some dimensions antitrust because you're going to be affecting the economic relationships. So it looks like if something is going to happen there, there has to be some leadership.

>>AVIVAH LITAN

It really comes down, in my mind, to economics. And if you look at what the FFIEC did with bank authentication, I didn't see any banks run out and buy smart cards and tokens. They've got the fraud problem under control with software and knowledge based authentication, cookies. I'm sure some people will argue that it's not under control, but if you look at it economically, it is. It's a very small piece. But when you get into these TJX situations, it's not a clear economic case. And in fact from TJX's perspective, their shopping's picked up since the breach. So consumers don't pay attention to this. And they blame the banks, I think. They don't think it was TJX, they call you because it was your account.

>>AUDIENCE MEMBER

There was even a shortage of plastic in February in part of this replacement. It was just an incredible.

>>AVIVAH LITAN

So this is good business for the plastic card makers. Did anyone want to add anything?

>> MICHELINE CASEY

I'll just add one more comment with regards to a hacking incident such as that and knowledge-based authentication where that can play. It's actually a great play for knowledge-based authentication. Because if a fraudster were to take some of that identifiable information, a name, a credit card number and an address and go try to do something at another business or a government agency that is utilizing knowledge-based authentication, there is very little chance that they'd actually be able to pass that quiz with just those pieces of information. We have the ability, or those using KBA, have the ability to automate 80 to 90 percent of people coming into a website and the penetration rate is less than 1 percent.

>>AVIVAH LITAN

Yes, we have time for one or two more questions.

>>AUDIENCE MEMBER

Can you tell us what kind of cost a merchant is going to incur for the knowledge-based authentication per consumer coming in the door.

>>MICHELINE CASEY

It does vary depending on volume of transactions but on a typical implementation, it would be somewhere between $1 to $1.50 per consumer. Plus you have no maintenance cost or replacement cost. If you lose a card, obviously you're going to have to replace that. You don't have that same issue with KBA.

>>AVIVAH LITAN

But as a practical matter, and I'm here to be devil's advocate, if you stop someone in a cash register line and put them through a knowledge-based authentication, the person behind them will go crazy. And also those questions, it's a good step. Those mechanisms have already been phished. They're not perfect. Every method has -- (Inaudible).

>>AUDIENCE MEMBER

The time that I tried to go through a company called Trufina here locally, it asked me where have you not lived? But it listed three -- I don't know the investment property addresses of everything I've bought and sold over the years so I couldn't pass the test to do something simple.

>>AVIVAH LITAN

That happens also. There are pros and cons.

I think our time is up unless we have any burning questions. I'm sure you can ask the panelists during the break. Thank you for your attention.

>>NAOMI LEFKOVITZ

Okay we will take a break and start back up at 4:00. Thank you.