FEDERAL TRADE COMMISSION

I N D E X

FEDERAL TRADE COMMISSION

In the Matter of:)
GLOBAL-E MARKETPLACE) Commission File No.
) P994312
----------)

Tuesday, June 8, 1999
600 Pennsylvania Avenue
Suite 332
Washington, D.C. 20580-0000

The above-entitled matter came on for discussion pursuant to notice, at 2:15 p.m.

APPEARANCES:

ON BEHALF OF THE FEDERAL TRADE COMMISSION:

DAVID MEDINE
and
JONATHAN SMOLLEN
and
HANNAH STIRES
and
ROBERT PITOFSKY, CHAIRMAN
and
SHEILA ANTHONY

and

MOZELLE THOMPSON, COMMISSIONER

Federal Trade Commission

6th Street and Pennsylvania Avenue, N.W.

Washington, D.C. 20580-0000

(202) 326-3505

P R O C E E D I N G S

- - - - -

MR. MEDINE: Good afternoon. I'm David Medine of the Federal Trade Commission, and John Smollen and our panel here. And obviously we have a good core of people who truly understand the importance of authentication. And obviously you guys are way ahead of the curve with everybody else, so we appreciate your being here. And we do hope to have a good and lively discussion about how communication is important to consumers.

We're going to break this session up into three parts. The first of three demonstrations is how authentication works so we can get a good working knowledge of a variety of authentication tools.

The second will be a broad discussion of authentication issues including cost, convenience, liability, and then the last part of the discussion will be how does this all apply and make sense and become necessary in the international context.

So to start off we'll have three presenters today. The first presenter is Russ Schrader from Visa. He's assistant vice president and assistant general counsel and responsible for managing legislative and

regulatory issues.

MR. SCHRADER: Thank you. Thanks. Since we're just back after lunch, I'll try to set the stage for the discussion here. We spent the morning talking about a lot of the benefits of E-commerce, the operational cost, efficiency to reduce cycle time, the accessibility, the low costs of the network, the global reach of it.

We talked about business opportunities in E-commerce. There are a wider range of things that the internet can do. Government filings, procurement, supply, auctions -- the Ebay presentation is particularly thorough -- content, delivery, payment and bill presentation, securities trading -- a lot of E-traders obviously are at the conference today -- but there still remains a single issue. And we'll take it

identity authentication, integrity of the networks, nonrepudiation consistent with each application. Maybe it's the payment guarantee. Perhaps there are other risk management tools, such as interoperability, convenience and global acceptance, like perhaps a brand that's widely recognized as a trusted brand for payments.

So let's move on to the next slide, and when you try to establish trust in a virtual world there's several different ways you can do this.

One is through authentication, encryption, digital certificates or digital signatures. I'll go into a little bit of each one of those. Now, the easiest is encryption or authentication. Are the parties who they say they are?

We're familiar with that today in our everyday booting of a computer when someone asks for a user ID or for a password. When you look at basic encryption, it goes back to a little kiddie decoder ring where you may have a symmetrical key, where both parties are using the same key or it may be a much more tricky one. We use asymmetrical keys, public keys and private keys as digital signatures and certificates that help you represent existing relationships and help you understand who it is that you are dealing with.

Look at the next slide. When we talk about that, there's the people and then there is the channel: How do you know that the message you've sent is the same as the message being received? Where for authentication it is, how do you know that the people that you are dealing with are the people that they say they are?

When you're sending a secure message and

into a relationship.

In the case of Visa and the SET I'll talk about, it's a banking relationship where identification can be endorsed through trusted third parties. It could be banks. It could be Visa. It could be Idenitrust. It could be Verisign. It could be any hierarchy of trusted parties that help establish this identification and who will stand behind that trusted identification. And also, this does leave a little less potential for fraud.

you are trying to do. You can have a client based digital signature that you could use with SSL. You can have other kinds of protocols and other kinds of digital signatures and encryption devices, but what SET was devised for in the payment system, in the joint payment system was to create an open specification for secured payment cards over an open network. And it was designed to reenforce an existing, trusted financial relationship.

You will find on the next slide a little bit

transparent to you when you got there and to the receiver, and then you would authorize as an existing Visa purchase order authorization through settlement.

There are clearly disadvantages to any of these encryption and authentication issues. There is still secrecy if you're using symmetrical keys and not asymmetrical keys. If you're only using one public code, that code may be stolen, and secrecy there is still a concern.

You need to determine that the public key truly belongs to the owner of the public key and that is basically the function of this certification authority, to come up with the authentication of the identity, or the other attributes that are represented by the CA. And when you have your digital certificate that sort of says John Doe, here is your key, here is your ID number, here is what you should have in order to do this, it's only as good as its issuer and the trusted relationship behind that.

In SET, that neutral trusted third party for certification is the banks. It's the bank who knows you who has issued your Visa card in my case, and it's the banks who is acquiring or working with the merchant. So I think that's kind of the background of authentication digital signatures as well as a very

brief explanation of how SET works.

MR. MEDINE: Actually we have four presenters. The next presenter will be Mike Baum, who serves as a vice president of practices and external affairs for VeriSign where he oversees the company digital ID and VeriSign Trust Network Operations.

MR. BAUM: Thank you. If you would permit me to wait until my slides get going, I'll pick up at the same time.

MR. MEDINE: Just while that's going on, let me say as a ground rule this morning's ground rule was that we are not going to focus on privacy issues. This afternoon's ground rule is we are not going to focus on the encryption debate. We'll leave that to other agencies and other forums. We will assume that there's adequate encryption to conduct consumer transactions and precede on that basis.

Mike.

MR. BAUM: Sure. Now, we'll get started. First of all I'm delighted to be here from Verisign and obviously these are important issues. There are vexing questions. Nobody has all the answers, to say the least, and so to speak, we're all in this together to make the environment better hopefully as quickly as we can.

One other initial comment is my time is quite limited today, so I had to decide whether to leave some slides in that I wouldn't necessarily have time to fully address to the extent that they will at least appear on the ultimate FTC web site if they'll have them. So I'll just race over a few slides, and we can always come back to them at a later time.

Next slide, please.

What is Verisign? I suppose other than talking about a Visa, everyone knows who they are, Verisign is this crazy thing called a certification authority that issues digital certificates and manages certificates. And it, in fact, goes well beyond that in terms of what we're doing today.

Next slide, please.

What we are effectively doing is establishing a global infrastructure of affiliates that correspondingly manage certificates within the scope of their geographic area or their service area. So effectively we are managing on a global basis a cogent set of policies to provide for interoperability on a global basis, and this is for a broad range of applications, some of which I'll be describing in just a few minutes.

Next slide, please.

What I don't have time to do is to get into a PKI 101 course right now, so I'm going to gloss over the next couple of slides, but suffice it to say that of course underlying the technology here is the use of asymmetric cryptology, which provides use of dual keys and can be used both for authentication and integrity purposes as well as for ultimately assuring confidentiality of information, all of which, of course, is a function of how it's implemented with respect to particular applications. Beyond that, I'm not going to jump into that slide.

MR. MEDINE: Mike, maybe if you could just maybe give the beginner's view just so people understand briefly how the public key, private key interact in terms of --

MR. BAUM: Certainly. There is at least one noted scientist on this panel. So if I get it wrong, correct me. But again, just at the highest level what

Effectively what it is is a public and a private key. The private key, which is one of the two components, is generally understood to be private by you or by your organization. It's a function of how it's implemented. It's secret. You never tell anybody that key. What you do is you use that key to create what are called digital signatures or alternatively to decrypt messages, again depending on the algorithm that is used.

For example, if I wanted to digitally sign a document to Mark Bohannon, who is sitting on my far right, I would on my computer -- hopefully it would be fully transparent, but I would create a message and could basically click to sign it, enter in a pass word, whatever else, that would gain access to the private key that sits on my computer or on some type of a hardware device, such as a Smart Card. It would bait the computer, then, using that private key and using information from the message itself would create a transformation called a digital signature.

The digital signature, again, is just a number that's unique to the message and largely unique to the key that I used to create it.

So on every message that you create you would have to theoretically have a different digital

signature. So over your lifetime you may have, again, theoretically, an infinite number of digital signatures. It's very different than a PIN or a pass phrase that is not typically dynamic. If this were disclosed over the net, of course, it would be a great security violation.

So some of the interesting characteristics of this technology are such that when I create a digital signature and append it, say to a contract or other message that I send to you, that anyone, including an interloper or a bad guy, if you will, could grab that digitally signed document and having that digital signature attached to the message. It would not do them any good. They would not be able to modify the message, such that the recipient upon proper verification of that message would not be able to determine that the message had been modified since the time that the digital signature was created.

MR. MEDINE: And the converse of that is that the recipient of the message can know with a high degree of certainty that one and only one person could have created that and that is the one person that has that private key?

MR. BAUM: Right.

MR. ELLISON: What it knows is that one and

only one private key created it.

MR. BAUM: And Carl will tell you later that of course one of the issues is, in fact, a critical for requirement for the use of this technology is that the private key of the originator remains secret to him or whoever the owner or appropriate user of that code might be. If that key is disclosed, of course, then you can't trust the message. It's pretty obvious.

We'll move right along to the next slide, which I will not get into for want of time. But basically there are two boxes there. The one on the left shows that basic function of a message in the key being the two key critical pieces of information that create the digital signature and then on the receiving side basically going through the process of verification. The bottom line is if the recipient has a true copy of the public key. Remember I told you you had a key pair, a public and private key pair that have a unique mathematical relationship to them.

So the public key, if it's properly distributed, and that's a whole other discussion we'll be getting into, but provided the recipient has my corresponding public key or more importantly Mark Bohannon has my corresponding public key, then he can verify that message that I sent to him and

determine that it did, in fact, come from me provided that my key had, again, been properly secured.

MR. MEDINE: Just also to clarify, it sounds like it's serving two purposes. One is to verify the identity of the person who inputs or is using the private key but also to assure that that message in its entirety is the message that that person sent unaltered.

MR. BAUM: It provides integrity assurance of the message. If you changed one single character in that contract, the digital signature would not verify by Mark, and therefore, he would know that there had been something wrong with that communication, and then he should therefore probably not trust the message.

And, again, depending on the algorithm used, you can also use this analogy not just for authentication purposes, but also to secure the confidentiality of communications, such that if I wanted to send Mark a secure message that only he would be able to read, provided -- and if I knew his public key, I could encrypt the message in his public key and that would only be able to be decrypted with the corresponding key which to the extent that Mark was the only person that had his private key, he would then be the only person that could decrypt it.

So it's a very powerful technology and one of the messages you'll see that I raised later is that when you think about the possible relation of this area, and we must also recognize that the use of this technology and certification infrastructure for confidentiality purposes is very real and very powerful and simply may have a different set of requirements from the regulatory perspective.

Next slide, please.

So I said before that if I were to send Mark Bohannon a message, then it was critical that he, in fact, had -- he knew what my public key was so that he could properly verify it. How is it that he would know what my public key was? Well, of course, I could have met him in a bar somewhere and if he knew me personally, I could hand him my public key and then he'd have confidence that it had indeed come from me. But realistically, and again thinking through what type of commercial infrastructure is being considered or employed, one more efficient method of doing that is through the use of what are called digital certificates.

A certificate is no more than a digitally signed data file that contains certain information and perhaps at a minimum it would contain my public key.

It may or may not be associated with my name or some other attributes, but at least it would contain my public key and would be signed by a certification authority or some entity that you trust.

So if Mark had my certificate to the extent that he could verify the digital signature on the certificate, it would be a digital signature of some

messaging and related systems. Next slide.

So what are the use of these digital certificates and the use of digital signatures and this technology? Well, you've heard Visa talk about the use of the technology in terms of the payments and, of course one of the protocols -- well, it's taken off more in Europe than it has here, but it's this protocol called SET that he mentioned represented in the lower left-hand corner.

Another protocol that you've heard from the professor from Utah, I believe, earlier today, he mentioned, well, if the little lock closes on the computer, the little key comes together on your browser, and that typically is an indication that the SSL protocol, secure socket layers, it was mentioned earlier has been used. So that would be provided for an end-user being able to authenticate a browser or who was operating the browser. And there are many other applications, including just simply secure E-mail, virtual private networks and a host of other applications that just continue to crop up.

Next slide, please.

One of the key points that I want to make today is that when you think about a certification authority, do not think about it in a monolithic

fashion. One size doesn't fit all. If you're going to think about regulating certification authorities, remember that Microsoft is even putting out a product right now that allows anybody to become a certification authority. So grandma could be a certification authority for her knitting club. So how will you ultimately regulate or put out regulations in terms of trustworthiness or other related requirements when it's being used for even communities of interest, if you will, that may be as mundane and as voluntary and as nonprofit, if you will, as a knitting club?

I won't run through the other options, but just as long as you understand that the nature of certification and the types of certification authorities that will be out there will range from government to private sector to informal to more formal to whatever, and it's really a blooming of a thousand flowers out there.

Next slide, please.

The other point to make is when we think about certification authorities, again, from another perspective, don't think of them as monolithic authorities. That is, it's not just a single entity that is evaluating someone's credentials or other information to make a decision as to whether

or not to issue the certificate to that person or entity. Instead, one of the things that we can observe in the industry is at a minimum a bifurcation between the back end of the certification infrastructure and front end up, such that the front end might be what is often called a registration authority.

You can think of a registration authority as just the entity that decides whether or not somebody should be approved for issuance of a certificate. It could be the Department of Motor Vehicles that makes that decision, but once it makes the decision, it sends the actual certificate issued over to an IS -- an information systems resource within the government.

From the private sector, it might be a company such as Verisign offering given corporations the ability to set up a registration authority using a browser on their site to make the decision as to whether or not to issue certificates to employees, but then sending cryptographically secured approval messages to Verisign who actually issues certificates.

So we need to distinguish between the entity that issues the certificates physically, and the entity that actually undertakes the registration.

Next slide, please.

And going beyond just a notion of

certification authorities is this notion of a PKI or a public key infrastructure, and there's a definition of it up there. From the internet space you can think of it simply sitting on top of or using the internet and ultimately supporting many different possible applications.

Next slide.

And when you think about the notion of a PKI, or for that matter even a certification authority, it is a lot more than just a piece of software. And those are at least a few of the attributes that perhaps a modestly trustworthy certification authority or series of certification authorities within a PKI might, in fact, want to have in place.

So, of course one of the tough issues both for government and the private sector is ultimately how do we assess the trustworthiness of these infrastructures. And at least on the back end those are some of the features we may be concerned with.

Next slide, please.

Now, a few paradigms over the next couple of slides, again, just for the purpose of perhaps modestly thinking through some of the issues that one might want to think about if indeed regulation was ever contemplated.

The first certification authority is not necessarily just a freestanding entity doing something just inherently new, but effectively think about it also as an overlay or enhancement to the existing infrastructure, perhaps one of the better examples would be what Visa mentioned to the extent that they go off and they spin up a SET implementation or secure electronic transaction and people are then sending their credit card information using this technology.

There's already a whole slew of regulation out there. Regulation of what, reg E and Z, whatever, would be fully applicable and already in place. So the mere fact that you're now using certificates is not necessarily an indication to think through a whole new regulation scheme just merely because you're using the technology.

In fact, the argument in that case would be what you're doing is even simply enhancing the security of preexisting systems. Another issue is that, again, we're not only talking about authentication in terms of what certification authorities do as I mentioned earlier, but also that they can be used for confidentiality. And if they're being used for confidentiality, I think a different set of paradigms

might apply.

Since applications vary, so might the regulations. We held a consumer workshop or a workshop that considered some consumer issues with PKI recently, and that was perhaps the strongest message in so many words. You have to look at it on an application specific basis. And as Carl may or may not opine on later, there's an issue as to whether or not certificates should ultimately provide for some assertion as to an individual or a company's identity versus their authority, and there's lot to be said for the use of certificates for many other different purposes; and clearly there's tremendous benefit, probably growing benefit, for the use of certificates to make assertions about the authority of someone.

For example, are they authorized to practice law? Do they have the right to write checks for their companies or whatever? But the real bottom line is, hey, the certification authorities out there to some extent will issue certificates as a function of market demand. And like it or not, the reality is that the market demands right now are for identity or identity-like certificates as well as authentication certificates. So again, let a thousand flowers bloom.

Lastly, not necessarily a message

intermediary. When you think about any kind of a regulatory scheme with certification authorization, don't make the assumption that they're involved intimately with every single transaction. Certification authorities under some paradigm could issue certificates and never touch or have anything to do with them unless there's a revocation issue. And I'll get to that a little bit more later.

Next slide, please.

There's also then continuing on this point, on this nontransactional model, when you think of Visa, or a similar payment mechanism, every time a consumer takes the credit card, it is likely going to be done in this country, it will be an on-line approval or an authorization for use of that card. But it turns out that when you think about CAs, yeah, there are models where that may invariably be the case, but there are other models where they're not involved in the transactions. And what I'd like to urge is there may, for appropriate transactions, be clear consumer benefits. And let me tell you what they might be.

First off, enhanced privacy. Gee, now a consumer can use a digital certificate to send an authenticated message or a confidential message and the certification authority will never know.

Nobody will have access to that content or message except the end parties.

Or, over here, facilitates unlimited use. Once the certificate is issued under some models, unless they are regulated out of business, the consumer can send effectively an infinite number of communications with that certificate, whether to authenticate or to make that information confidential. And they're not going to be hit up with a 2 or 3 percent fee for every transaction, okay, or at least a corresponding merchant. So again there is an economic potential benefit.

And lastly, I grabbed the last ones there. Again, this notion of unlimited use.

Next slide.

One more important paradigm, if you will, before I quickly move on to a number of other issues. There's been a tremendous thrash among the pundits as to the propriety of open versus closed systems. And the whole notion here in part while there are many different definitions for open or closed, the notion is that if something is closed, it's, you know, it's a very intimate community and everybody has got a contract signed with all the parties and everyone knows their rights or obligations.

Unfortunately, I would claim that the discussion typically on open versus closed turns out to be no more than an eloquent set of fighting words, because effectively what we've seen is that many systems will effectively by way of web rats are ultimately on-line providers for allowing a user to contract and effectively become part of, if you will, a very large or more dynamic closed system.

Next slide, please.

On the whole area of private key protection, there's not a lot of time to get into it right now, although perhaps this may come up later during the discussion. But the point I'd want to raise is that for so many systems with the tens of millions of browsers that are out there, that consumers are really primarily using, those are not necessarily owned, operated or controlled by certification authorities.

They're owned, operated or controlled by the Microsofts, the Netscapes, or the other manufacturers. And the question is where are they at this table? They ultimately control that piece of software, have the greatest amount of control over the interface, the greatest control over whether or not the cryptomodules that hold the private keys are, in fact, protected. And it's very important that we think about those

parties in the broader schemes of rights and responsibilities.

Why don't I move on to the next slide?

Also, by way of Verisign, for example, offering consumers enhanced mechanisms to protect their private keys are important. And here is at least one of our web pages where in fact we are offering Smart Cards to consumers if they want them to enhance the protection of their private keys.

Next slide.

Also, of course, the notion of trust credentials. How do you know which certification authorities to trust? Well, I hope there will be a discussion at some point of mechanisms for assessment on a very broad global basis. But for want of that, some of the criteria or attributes of trust are some of the things listed there. And I claim that one of the big ones is a very rigorous recognized, detailed audit of the infrastructure, and there are many different -- there are an increasing number of programs where they ostensibly provide these types of audits, but it's an audit not only where you have purportedly good procedures, but indeed whether you are following it, which is the second half and the much more costly half; and that means a fair amount of work. Why don't I just

keep moving?

The last point I wanted to raise where it says future. Browser Root Policies. One of the interesting things going on that one can observe over the last six months to a year is that the major browser manufacturers are now setting criteria for the certification authorities to actually include their public keys, their root keys, in the browsers, and I think you're going to start to see more focus on what those criteria are as a gatekeeper of trustworthiness that, of course, will affect the consumer in its use.

Next slide.

Offering enhanced insurance has been raised by other speakers at this program today, and, of course, Verisign offers the Netsure Protection Plan, which was the first one, I believe, that was out there offering enhanced warranty protection to users.

Next slide.

Just to mention, there has been a lot of work in this area, and while not every one of the provisions and paradigms listed in these -- the guidelines that are up there and now the work on the PKI assessment guidelines -- will necessarily be agreeable to everyone. The bottom line is as we begin to think more about the rules and the problems out there, it's at

least worth taking note that there is a fair amount of work being done out there in the field right now.

Next slide.

Again, to wrap up, I did want to notice one interesting initiative right now. While, of course, the use of disclosure technologies and disclosure from a consumer perspective is certainly not adequate, and I've learned that from some of the experts in the field, it certainly is at least an important step; and in that regard one thing I can announce today is there has been a fair amount of progress made in the development of a succinct, brief proposed model disclosure statement for PKI's that can be used either by freestanding PKIs or by even existing companies simply deciding to deploy this type of technology.

What you see listed up there are some of the issues that seem to review -- to actually move forward. I'm just about wrapping up now. Next slide, please.

Now, just to mention there was with the information security committee of the ABA workshop on

And also just to note that just last week among representatives of the PKI industry, there is now the go forward and will likely be a press release quite soon establishing finally a PKI industry association. And I know regulators always like associations so that they can get some kind of industry-wide accountability.

Next slide, please.

I'm just wrapping up with some references, and those are the end of the slides. Again, thank you for your patience.

MR. MEDINE: Thank you very much and that was extremely helpful in educating us about some very complex, technical issues.

We are very lucky to have our next speaker here, Carl Ellison. You can imagine when the Federal Trade Commission called Intel and asked one of their employees to come to the FTC hearing room, that caused some apprehension back at home. Carl was willing to come nonetheless, and we appreciate it.

MR. ELLISON: Thank you.

MR. MEDINE: He's a security architect for Intel.

MR. ELLISON: Thank you for the opportunity to come here and talk. You're correct. When they told people I was coming here, there was a great deal of

apprehension and then I told them why, and they relaxed.

I'm here to talk about some security concerns that we have that we need to have when using digital

The old check-writing machines impressed me as a child. My father had a small company, and that company had a check-writing machine, and I was, I guess, five years old, and I loved to see this thing. And I talked him into letting me stamp a blank piece of paper one day, because it made all these pretty raised bumps in red and blue. And it had all these levers for numbers and this big wooden handle that you pull down to go ca-chunk and write a check with it.

What I've learned recently is that these machine signatures are not valid. There's case law apparently -- I'm not a lawyer, but I'm told that there is case law to the effect that these signatures are not valid.

Next.

with an embossed number, there's nothing in that tells you anything about who pulled the handle. So there's nothing you can take to court to show who pulled the handle.

Next.

But if you have a contract between the owner of the machine and the bank, you don't need to prove who pulled the handle. The contract will say that the bank honors this and the owner of the machine will not dispute it.

Next, please.

The problem we have today is the digital signatures are less secure than the mechanical signatures of that check-writing machine, less secure in spite of the fact that they have these wonderful property that if you change one character, the signature is no longer valid.

The first reason they are less secure is you do not know who pulled the handle. In this case pulling the handle is pressing enter on your computer. You don't know who pushed that key, and you have no evidence about who pushed that key that you can take to court.

Next slide.

Another problem we have with public key

technology on a digital computer is that my father put his check-writing machine into a locked safe, and he would take it out -- once he took it out to let me play with it -- but he took it out only when he was going to write checks, and otherwise it stayed in that safe. But a digital computer is too expensive and has too many uses to be put in a safe except when you're going to take it out to write checks. The exception to this might be the computer that Verisign uses for their high value keys. I've been to Verisign. I've seen the safe that they keep it in.

So in that case -- in some cases you do put the computer in a safe and you do protect your keys that way, but in general you will not be putting the computer in a safe.

Next bullet.

And what's worse is the real handle that you pull is not this big wooden handle that I had a tough time with as a five-year-old. It is, in fact, not advisable to the user. It is just software, and it can be fooled by a virus. You know, Melissa 12, whatever the virus is that will come out and will go around signing things, with private keys that it discovers. And that kind of attack, the virus attack, is not noticed by the person who owns the private key, so you

can't even report that something went wrong. It's not as if his credit card or smart card was stolen. The smart card was still there plugged into the machine. At night he takes it out of the machine, puts it in this pocket and goes home. But Melissa 12 signs something with that smart card without his knowledge.

Next slide, please.

Now, I claim that businesses can still use digital signatures and use them well because -- and we'll go through a set of bullets.

Next bullet.

Specifically, you can do business to business EDI based on a contract between the two firms doing the business, the same kind of contract that made a mechanical signature valid can make this digital signature valid between these two firms.

The next is -- we can just do the rest of the bullets. The business can put its digitally signing machines under surveillance and can watch their use. It can put locks on machine rooms and locks on the purchasing department office.

It can use secure work flow for high value signatures. Secure work flow is a process that we are working on in Intel and a number of others, I'm sure, in which you have multiple parties that have to be

involved before a signature will be made. And each of those parties authenticates itself to authorize this final signature.

You can have single-use machines in a business. You wouldn't have that at home. I mean, it might be nice if everybody went out and bought a separate computer for every function. That would be a lot of Intel chips. That would be nice, but that's not going to happen; but it might happen in a business.

Furthermore, businesses have fire walls and other network security, hopefully to prevent Melissa 12 from coming in and doing digital signatures, and the final bullet. Businesses often, at least Intel does, as I'm sure that most businesses do, have a policy against loading strange code on your machine, code that might introduce viruses.

Can we go to the next slide?

There is a place, I believe, for home user signatures. The first would be low risk applications. For example, I have -- my bank offers me a web page that let's me move money between my checking and my savings account, I would be very happy to authenticate that by digital signature. Right now all they let me do is passwords. I'd much rather have digital signatures for that, but that's a low risk application.

The most that can happen is the inconvenience of having my money in the wrong account. No one can move money out of my account into their account with this mechanism. Or I can do purchases under the credit card mail order telephone order rules, because those are relatively low risk. Under those rules, I can dispute line items on my credit card statements, and I am assumed correct until the merchant provides hard evidence to the effect that the transaction really did occur.

And, of course, we can always use signatures on home machines for known value applications, signing E-mail or authenticating access to personal web pages. These are applications of so little value that they would not be attacked anyway, but I would be very nervous about using a home computer for any high value digital signature, because we will not see the protections on the home computer that a business might be able to put into place. We will not see single-use machines. We will not see machines in access-controlled rooms. We will not see machines under video surveillance. We won't have fire walls. We will not have provisions against downloading strange code. If you have a teenager in the house, you know first thing there's going to be a lot

of strange code downloaded on this home computer.

So we go to the next slide.

Now, I've got two more slides, and these are a short quiz on computer security that I wrote. I will ask for a raise of hands, a show of hands for this quiz.

The first slide, and this ties directly to one of Michael's slides, and thank you, Michael, for introducing this. I have in this model two different computers. The left column is a desktop computer. It might be at a business. It might be a home computer. You know grandma's knitting club computer or it might be some, you know, IT computer at work, but it's a normal desktop computer, and it's not specially protected. It's not in a locked room. It's not under video surveillance, so it's reasonably attackable. But on the right we have the ultimately protected computer. This is in a locked room with video surveillance, with strong personnel procedures, probably multi-party access control so you have to have two or three persons anytime you get near this computer. So I've got three cases for issuing certificates.

Case A, the certificate is issued just by a certification authority in that Fort Knox.

Case B, it's issued by the CA in Fort Knox, but on direction from a registration authority held on the desktop.

And case C, it's issued by a CA in that desk top machine.

And in black print I show where the client is, the client for whom the certificate is being issued.

In case A, the client is on the phone or the net talking into Fort Knox.

The in case B and C the client is at the desk, at the desktop machine.

Now, the question is which is the most secure?

I'd like a show of hands who thinks A is the most secure. Nobody. Okay.

MR. MEDINE: One.

MR. ELLISON: One? One thinks A is the most secure.

Who thinks B is the most secure? Four? Four.

So one, four, and who thinks C is the most secure? One, two -- seven people in the room.

MR. MEDINE: A lot of abstention. There should be a fourth opportunity to say it depends.

MR. ELLISON: It depends.

MR. MEDINE: Or I don't know.

MR. ELLISON: Actually, I claim it does not

depend. My answer is that C is more secure than B, and B is more secure than A; and I put this slide up on purpose because this is counterintuitive.

The reason that A is less secure than either B or C is not a security problem with Fort Knox. That CA is solid. The key that's used in that CA is well protected, will never be revealed. The problem is this client is on the phone or over the net, and it is very easy with no security or crypto expertise at all to engage in identity theft over this phone connection. Run of the mill criminals know how to do that today, and so the easiest attack anywhere in that system is the attack on A.

Now, B and C don't have that attack. My assumption there is the operator of the desktop machine knows this client. You know, it might be my bank for example. He knows me, my branch bank who knows me or it might be my IT department at work who

The first question for electronic commerce, it's been said occasionally, although I haven't heard it yet today, that electronic commerce needs the deployment of a PKI in order for it really to succeed. How many think this is true? One.

How many think this is false? Seven. Okay. That's good, because I agree with you there, and the evidence for that is there is no real PKI yet and electronic commerce is succeeding just fine.

Next section.

And the next one is -- this is the last one, last part of this quiz -- we know -- and before going to Intel I was at Cybercash as a cryptographer for Cybercash where I dealt with this specifically -- we know the computers need security in order to do -- in order for electronic commerce to succeed. We keep hearing this from consumers. We hear it from surveys. We know this is true.

What is the best way to give them security? And so multiple choice. Answer A is strong cryptography, and that, of course, is my favorite as a cryptographer. This is what I really want to believe.

And number B is laws that guarantee nonrepudiation. We have heard occasionally about nonrepudiation. Russell mentioned it. Nonrepudiation

means that -- Michael, maybe you can define it better than I could.

MR. BAUM: Sure, Carl.

There's the notion of nonrepudiation. It's sort of a legal term, but the notion there would be that -- and by the way I -- with full knowledge I'm being set up for Carl. I will blissfully participate in this exercise.

Basically what nonrepudiation -- the notion of it there is that your transactions that you create will be -- you have a high degree of confidence that they will be enforceable. Okay. And one notion -- in fact, the first use of that term in the context of even the predecessors to electronic commerce, was actually by security experts with no legal backgrounds. And they basically presented it as though there is nonrepudiation or there is not nonrepudiation, and they presented it as a security service. The better way, perhaps, to look at it wa18 T diegT* úúú 3

system, and if a given digital signature is received by the recipient that, in fact, the originator, subject to a number of conditions, would be held to have sent that transaction. That is where it is. Now Carl, since I've greased the slides, go for it.

MR. ELLISON: Thank you, very much. I should mention that you're on a panel with me every time I talk. And the third option is laws guaranteeing repudiation. I had to throw that in, right?

How many vote for A? One. Only one?

How many vote for B? One, two, three, four.

How many vote for C? One, two, three.

MR. MEDINE: How about none of the above?

MR. ELLISON: None?

MR. MEDINE: None of the above.

MR. ELLISON: No. I didn't give you that choice. I mean, I have spent my entire life in school with multiple guess questions where I wasn't given fourth choice. I'm not going to give it to you.

So I'm voting for C, and the reason I'm voting for C -- I had this discussion with a few people upstairs -- the trick here, the thing that disillusioned me when I first got into E-commerce when I was at Cybercash and for that matter the reason that I'm now with Intel is that what we found out was that

consumers don't want securities the way cryptograms define security. As Michael has said, nonrepudiation was a term that came out of the cryptographic community, and it was a term that I heard bandied about by noncryptographers. And it's a case that the cryptographers should have kept their mouths shut, I believe, because, what we really discovered was what consumers want is power over their own money.

They want control. They don't want security the way a cryptographer defines security. Absolute privacy or as close to absolute privacy as you can get, confidentiality. The kinds of things that we worry about when we design systems that could be good enough to control nuclear weapons, the things we worry about are not what the consumer wants.

The consumer wants the ability to control his own property. And he's got that ability already, with credit cards he's got it in reg E and reg Z and reg E and reg Z are answer C up here. This is a regulation that allows the consumer to say, no, I didn't buy that. It allows the consumer to repudiate some action, and to me as a cryptographer, I wanted A myself.

My community of cryptographers encrypted the discussion around B, so that would have been my second

guess. So what I learned from the consumers, from the world, was that the answer was C.

MR. MEDINE: Thank you, very much, Carl. We have now have had our hopes raised and our hopes dashed by PKI. But we'll have perhaps a later discussion to clarify that.

I just want to mention that Hannah Stires is here as well from the business practices, and she and John have been integral in bringing together this two-day event. I want to recognize their work and move on to James Wayman, who is the director of the U.S. National Biometric Center. So we can get an idea of a way to authenticate.

MR. WAYMAN: Thank you. I appreciate that. Can we have the slides? It's listed under -- Wayman 99 is the name of the file.

I'm Jim Wayman. I'm a director of the U.S. Director of U.S. Biometric Test Center. We are financed by the federal government to study federal applications and state applications, too, of a biometric identification.

We advise on the performance and design of government systems, so we stay out entirely of the commercial arena. We don't get involved in how biometrics may or may not be used in commerce, nor do we get involved in how biometrics may or may not be

used by individuals.

So when John Smollen called me up and said would you be interested in doing the conference? I said, I have to tell you, this is really beyond the scope of what we're involved in, but nonetheless I thought I would come and lend my two cents worth, because I do know something perhaps about the area of biometrics, if not this particular application.

There is a federal government interest site, funded by both the DOD and the MIST, that's www.biometrics.org. If you go there, you may have to click a couple of times, but you will get to the National Tester Center. And I'll get to our web page, and you can see the kinds of work that we've done, primarily in the area of the mathematical and statistical evaluation of test results and system performance prediction.

Next slide, please.

If we're going to be talking about biometrics, we need to supply a precise definition of what we are talking about, so we used this one, the biometric identification is the automatic identification or identity verification of individuals based on behavioral and physiological characteristics.

By automatic, we mean that this identification

always occurs using a computer and in real time. You may be interested in DNA analysis, but we are not. DNA analysis is a laboratory technique. It involves human intervention. It's not done automatically. It's done in real time, so I don't know anything about it at all.

I'll talk in a minute about the difference in identification and identity verification. But if individuals -- I've left out the word living individuals. We presume you have a living individual in front of you. We're not interested in identification of dead bodies or anything like that.

physiological structure, but your behavior, as you know, greatly influences the face that you present to a sensor. So we know that all biometric devices operate on the basis of both behavior and physiological characteristics.

Next slide, please.

Now, what I found intriguing about Michael Baum's presentation is that he talked about the two ways that you can use this asymmetric public, private key pairs. You can run them forward or you can run them backwards. You can run them forwards by encrypting with a public key, and therefore the receiving with his own private key can decrypt the message, and you can have secure communication.

You can run the key pair backwards, and you can encrypt with the private key and use it as a digital signature.

Well, biometrics works kind of the same way. You can run these things forwards or you can run them backwards. There's two ways, different ways, of looking at this thing. You can use them for positive identification to prove I am who I say I am. At least this is with respect to a roll identity on the data base or you can run these things backwards to prove I'm not who I say I'm not.

The purpose of positive identification is to prevent multiple users of a single identity. I would think that in electronic commerce, that's primarily what you're trying to do. You're trying to prevent someone else from using my identity in a commercial transaction. But what we kind of really fear is biometrics thrown in the reverse and negative identification to prove that I am not who I say am not.

Now, believe it or not, a negative performs the largest form of biometric identification in use in the world. In the State of California where I live, you have to give a right thumb print to get a driver's license.

The purpose of that is to prove that you are not anyone who has previously had a driver's license in the State of California under another identity. The purpose of negative identification is to prevent multiple identities of a single user. To prevent me from getting multiple licenses in the State of California under multiple identities to prevent welfare multiple recipients receiving multiple benefits under multiple identities, to prove I am not who I say I am not.

I want to add one more thing about positive identification, and that is ultimately biometric

identification can never establish who I really am, only that I'm not the same person that presented myself earlier on for enrollment. How do I really establish -- I had a lie detector test once. And they kept asking me if my name was Jim Wayman, and after a while I started to think, how do I really know that my name

You know that your height changes during the day. I guess they say you're tallest when you first wake up. Your weight certainly changes as your hydration state changes during the day. Everything about you changes during the day. And one of the problems about biometric measures is that they are not very repeatable, and they are not very distinct. You object to that. You say Jim, for crying out loud, I have read so many murder mysteries, I know that fingerprints never change.

Can we have the next slide.

Well, here is the same fingerprint taken off an individual at an interval of less than six weeks. I don't know which fingerprint was taken first. I think the one on the right was. About -- I might add that we've tested about a dozen of the biggest and best fingerprint algorithms in the world. None of those algorithms have been able to successfully detect that these two fingers match. About 3 percent of the fingerprints that we've collected in our standardized test data base -- we've got about 3,000 fingerprints -- about 3 percent have levels of destruction comparable to this one, and they cannot be matched by even the best systems in the world.

The fingerprint that you see on the right is a little bit over moist. It's a little bit too dark in

some areas, and there is some blurring of the ridges. The valleys seem to be gone. The one on the left is a much better quality image, but the fingerprint itself is kind of gnarled, chapped and scraped and broken. So you can see that your fingerprints aren't necessarily repeatable. So I learned a new word this morning. Maybe you did too. That is this GUID, was that the global universal identification? If you are looking to biometrics to supply the magic GUID, global universal identification, it's just not going to happen

That's not what these devices are going to be used for, because you enroll with the fingerprint on the right, and then you come along and you present the fingerprint on the left. And there is no system currently in the world that recognizes those two prints are precisely that same from the same individual, same finger.

MR. MEDINE: Some people call it a GUID.

MR. WAYMAN: GUID? Is that what it is? That was a new word for me.

I thought I'd contrast for a little bit the difference between PINs, ID numbers, keys, and then biometrics on the next session. I certainly am not an expert on the first three, but it occurred to me that PINs are fairly stable. My PIN for my phone at work is

1234. I suppose that is not a very good PIN, but it has stayed that way, and it has not changed. You saw my fingerprint changed. My PIN never changes unless I change it. Unless I step in and intervene, my PIN remains stable. My PIN is replaceable. If I lose it, it gets compromised, I can just change it. If I get worried you're going to call up and start getting voice messages off my machine, I'll just go back and change that PIN. It is certainly is interceptible.

In fact, I just transmitted it in such a way that all of you intercepted it. But the PIN is primarily linked to the account. In fact, a woman that works with me as the administrator of the test center uses the PIN. She has it.

So it doesn't identify that I'm the one accessing the phone. She, in fact, would be accessing the phone, but it's a link to that phone account. That phone can be accessed by anyone who know the PIN is 1234. Only limited storage is required. If I forget it, I can write it down on a piece of paper, four digits, no big problem.

I guess you can you do that with -- I think in FAST. You can't do it with one byte, but you can do it with one byte and an extra bit. So the very limited storage required for a PIN. ID numbers. You can add

-- unique to the ID numbers -- what I might have said is that 1234 isn't very unique and if I probably asked around here, some of you in this room are using that same PIN for access to your account. So PINs are certainly not unique, but ID numbers can be.

In fact, my Visa card's number, which I won't give you, is unique. I've never had my Visa bill, unfortunately, sent to anyone else, nor have I ever received the Visa bill of anyone else. My Visa number is absolutely unique, and you can say all the other things about PINs apply to ID numbers. That's stable. My Visa number doesn't change unless I change it. It's interceptible. It's linked to the accounts. My wife uses my Visa number whenever she wants to. It requires more storage certainly than four numbers.

Now, the private key we've been talking about in an asymmetric system, we can add maybe nonrefutable. I can refute that I used the PIN. Oh, no. It was the office manager that used the PIN, and that would be true.

You might say it's nonrefutable. At least we know that that message was generated from that machine that held that private key. I may not know, as Carl mentioned who was running the machine, who pulled the handle, but at least I know that it came out of that

machine. And key isn't interceptible, because at least once you've transferred the key to the machine in question, the key doesn't pass around. You don't pass that key around. It sits in the machine.

So those, at least, are my idea of what PINs,

geometry, close enough at least. So your hand geometry is not terribly unique. A fingerprint -- some of the good systems do pretty well. We've done 16 million comparisons with only a couple of false matches.

One thing is interesting. There's a whole lot of people who have fingerprints that match fingers -- other fingerprints on their own hand. And maybe -- my rough guess is maybe one out of every 300 people have two fingers that match each other very, very well, at least by the standards of these automatic identification systems.

So you might try that next time you see a demonstration. You might see if can't fool the system into thinking that one of your fingers is another finger. That's a fairly common thing that happens.

Biometrics are interceptible. We don't see. I don't know understand this model that some have proposed that we're going to somehow have these biometric templates flashing around on the internet. I still haven't gotten that together.

People say we can encrypt the biometric template. It seems to me that's just adding another layer of indirection, and I really don't get that either. I don't think biometrics are going to be -- you said it was a GUID. They're not going to be our

GUID. We're not going to have these things flashing around on the internet. That makes absolutely no sense, because they can be interceptible, and if they are nonunique, they certainly can be refuted.

Now, there are a couple of things that are nice about them, however, and that is that they're linked directly to the person. If a person gives you a fingerprint and if this one here, you know if the person is me, it links the transaction to me. It doesn't link it to the computer that held the key, for instance, and lastly, the convenience of this. No storage is required. I can give a fairly detailed pattern on the face or my hand or my fingerprint or my eye patterns without requiring any further storage.

Next slide.

Well, is there, then, a use for biometrics in E-commerce, and I believe there is. And that's exactly what Carl talked about. You can take your computer, and you can lock it up in a safe. The other thing that you could do and is being done and is commercially available now is you can lock your computer up using biometric access. So your computer holds your private key.

Now, you don't know, perhaps, who is going to get on your computer. I keep my computer with me all

the time. At least I try pretty much to, and I figure if I ever let it down, it will probably be stolen. But there are methods by which that computer can be locked up so that no one but me presenting a correct biometric measure can get on that, on the computer.

Such methods are available commercially now, but authentication will be here on the commercial level. I'm authenticating to myself to my own computer, saying computer, you know me. I'm your owner. You can go ahead and release documents signed with my private key. So I release using the private key using authentication on my own computer or you might argue on your own local network. You might have some sort of a local network in your office where the biometric templates are stored at a local network level and signed on biometric authentication.

I have no trouble with that, but I'd like to see authentication at the user's option. I don't currently use biometric authentication to lock up my computer. I have that capability. In fact, there are -- you can download a voice recognition algorithm for 19.95 off the internet from Tianetics, for instance that will work right in your computer. It works on one of our computers in the lab. You can try that out if you want. At your discretion, at your option, you can

currently now, with existing technology, lock up your computer using a biometric signal so that only you can get on that computer.

You have control of the stored pattern. That stored pattern that represents my fingerprint or my voice print or my eye print sits only on my computer. It never leaves my computer.

There's a second model people now are talking about, and I believe that is going to happen in the next couple of years because I've seen all the hardware required. People are talking about embedding finger print scanners in the smart cards so that the smart card won't unlock whatever keys it holds until the correct fingerprint is scanned on the smart card. I believe that's a reality. I have seen enough hardware now that I -- and I've seen some prototype devices. And I think we're going to see fingerprint scanners embedded into smart cards.

So you've got the fingerprint templates stored on the card. You hold the card. The template never leaves the card. You have total control over your biometric measure.

Now, as you saw earlier on the slide with the fingerprint that was all beat up, sometimes these methods aren't going to work. So you have to install

a back door. In the case of fingerprinting, unless you're a portion of the population, maybe a percent or two that simply has such poor fingerprints chronically that you can't use fingerprinting, what we generally do is advise you to store two fingerprints.

And, see, your back door is the second fingerprint. If your right index finger doesn't work, use your left index finger. But in any case, there will be days when you simply are not yourself, and the back door is required to access to your equipment. So some of the computer makers that are talking about installing biometric devices at the bi-house level are also talking about installing back doors. Complicated back doors that prevents a thief from stealing your computer and going in the backdoor, but backdoors nonetheless that allow you onto the computer in the event that the biometric device does fail and biometric identification does indeed fail.

So consequently, I'm suggesting no mandated standards or controls. Why should the government care if I choose or not choose to lock up my computer using biometric authentication. And why not simply let the marketplace work this out or let the individual users work this out or let me decide which level of security I want controlling access to my

own computer. I can imagine some liability issues where you say to people, well, if you lock up your computer with a biometric access control device, we won't hold you liable for any charges that are incurred by unauthorized use of the private key for instance. I can see us doing that, but I don't understand the need for mandated government standards if we're only talking about access to my computer. And currently available technology is that we had to do this.

There are fingerprint devices that are being sold now embedded into keyboards. There are facial recognition devises that you can download from the internet, and pay, I believe, it was $135 for it last time I saw it. Now, for facial recognition devices, obviously your computer is going to need a digital camera, but I've been told by computer manufacturers that they expect most computers to come with digital cameras here in the near future. You can download the Tianetics piece of software for voice control at your computer using the built-in microphone that your computer probably already has. So these devices are already currently available.

So if you feel the need to control access to your computer using biometric devices, the technology is already in place. You can do that, and I'm suggesting

no further need for standards or mandated regulations.

contract. When that rule becomes changed, state law in almost every state law are when -- generally when the transaction involves either a large amount or an issue of such importance that the law has said we must have the contract to be written, otherwise regardless of the ability to prove its terms, it will not be enforceable.

An example of that is a real estate contract. Both parties may totally agree that the terms of a real estate contract are the same, but the law will not enforce it unless it's been in writing.

The standard is the statute of frauds. The statute of frauds requirement in most states say no contract can be enforced for a value of more than $500 unless it's in writing. And then you go on to parole evidence rules. You have authentication requirements, evidentiary rules when you are trying to prove something in court and so on and so on. What happens to, say, the statute of frauds when you have an electronic transaction?

The issue as to the validity of the terms of the contract when the entire transaction is electronically -- is conversed electronically becomes are the parties who they say they are? And is the terms of the contract as reflected in the electronic

reproduction reasonably reliable? And it is that type of analysis I think that we get into before we even need to talk about do we need a digital signature. I don't need, and I don't think I'll ever need, a digital signature for my e-mail with my office, which we have quite a bit. We have a Boston office, and we probably exchange a hundred e-mails a day, and we don't need digital signatures. But if I decide to buy some land in Montana, and I promise that Margo Saunders will pay $20,000 for these ten acres of land in Montana, I sure as heck want the person on the other end to know that they are really dealing with me, Margo Saunders, and not allow David Medine to promise that Margo Saunders is buying the 20 acres of land in Montana.

Now, I also don't need a digital signature so long as I'm using my Visa or my MasterCard, because under reg Z, I have the protections of the Billing Rights Act, and that law is not perfect, but it provides virtual protection so as long as within 60 days after I get my bill if I recognize that there's some mistake on it that I follow the rules. But that is about it so far as consumer protections in federal, and there's virtually none in state law.

So if I were to use my Visa, my other card in my wallet, which looks like a Visa, but is actually an ATM

card, and buy a book through Amazon.com and actually, and it's never delivered. I do not have nearly the degree of protection under reg E that I have under reg Z.

Now, I cannot complain that the book that was delivered that I was promised, as I can under reg Z. I can only complain that the amount that I authorized to be withdrawn was not withdrawn. And I have a much smaller amount of time within which to complain, and I have the burden of proof and the money is taken right out of my checking account for whatever account, the ATM card is tied to, and it stays out until I prove that, in fact, that I did not authorize that transaction.

So when we talk about authentication, and we talk about the degree of whether we're doing digital signatures or PKIs technology or biometrics. It all depends on what the purpose of the authentication is. And I think it's very important -- I think the underlying assumption has to be that we have built an

electronic transactions until consumers have the ability to repudiate transactions that both either were not really theirs or were not really according to the terms that they thought that they agreed to.

MR. MEDINE: Let me just pose that question to Russ, which is as Margo says, we have existing protections under Unfair Billings Act and regulation Z against improper use of credit cards. Why do we need SET? Why do we need digital signatures from the consumer's perspective if they already have those protections.

MR. SCHRADER: Well, I have good news for Margo. Provided that you used your ATM card, and it was a Visa, it was a Visa ATM card, on-line Visa debit card, you're covered.

Last year Visa adopted the zero liability policy. If there's unauthorized charges within the two first days, you have zero liability. Although you don't have regulation Z protections, you have the voluntary protections that Visa implemented called charge-back mechanisms. If that's not your book from Amazon or if it's defective charge, return it. That institutes the charge-back, and it will be handled through Visa's charge-back system. If you have a card that doesn't say Visa, well, shame on you.

MS. SAUNDERS: May I respond to that?

MR. MEDINE: Yes.

MS. SAUNDERS: The National Consumer Law

the issuers don't succeed in following the op regs, then Visa wants to know about it so that they can look at it, but clearly it is part of the contract that Visa and the issuing banks, requires banks, and the cardholder all vary.

MR. MEDINE: Can you just go back to my question? Why do we need SET if we have from the consumers' point of view if we have protections, repudiation? Why do consumers need authentication, encryption, digital signature technology if they have legal protections in place?

MR. SCHRADER: They do have legal protections in place. SET and all authentication issues, and I'm not just going to say just SET, because we've heard about a lot of other alternatives that could work easily as well, SSL and the rest of it. It's one additional layer to set the kind of environment that we have that allows Visa to make the kind of promises. We have been able to offer this kind after zero liability, because fraud numbers have gone down. Fraud numbers have gone down because of risk management tools, because of authentication, because of encryption, frankly, because of the help that the FTC has given us, this going after the bad actors. We've been working with your group as you know, in some of these web

merchants and shutting them down, and we appreciate that help. That's allowed us to make these kinds of market moves that has helped.

To continue to have authentication, whether it's SET or SSL, other kinds of encryption, it will just continue to make the environment more comfortable and reduce the level of fraud.

MR. MEDINE: Mr. Ellison.

MR. TORRES: Actually, I just wanted to jump in again, and I'll be talking a little bit about the payment question. But just to get back to the idea of debit cards and the voluntary liability and I think there's a panel tomorrow talking about self regulation, and I just kind of put that voluntary limits in it. The consumers' union had been out there with the NCLC and others and I think if Edward was here he would also relate some stories about how there's apparently been a failure in the way that voluntarily that program is working and why in some cases we do need some regulations.

I don't think they are in question on using other forums and why we need some of these other forums. If we've got the limited liability on the credit cards, there has been this push to use debit cards, then why this push for this other technology, and what's behind it, and how do we get consumers kind of geared up to

using those other technologies. If there is going to be problems with liability and problems with security and those other systems.

MR. ELLISON: Sure. This is -- maybe this is a bit -- and it may turn a lot of people off, and if you go to sleep through this, I'm sorry. Michael alluded to this. Margo, at one point I love what you were saying, but at one point you referred to knowing who was making this transaction, this land purchase, knowing that it really was Margo Saunders at the other end of that wire and not someone just claiming to be. And I think that's what we're talking about when we talk about authentication.

The trouble is we are accustomed, and in a way that law is accustomized to speaking of authentication by talking about people's names. You used your own name on that example. Michael was careful not to tie all those to names.

The SET example was my favorite example. The cardholder certificate on SET does not have the person's name on it. It's an entirely anonymous credential. It authorizes the key holder to use a given credit card, but that's all it does.

So what I think is important here, one of the things that happens with the internet that people don't

talk about very much -- I try to talk about it, and Michael knows I talk about it so he set the stage for that -- but one of the things that happened is that suddenly we have a community that is so large that the names we are used to using as identifiers don't work anymore.

I went all the way through school as the only Carl Ellison. So if someone wanted to refer to Carl Ellison, I knew they were talking about me and so did all my classmates, but I am farara`0 0on

fact, the point I was trying to make is that sometimes me, Margo Saunders of Virginia or Washington D.C., doesn't need to be identified on the internet. In fact, perhaps I would prefer not to be identified, but I may want to participate in some chat room, not really, but I may want to -- someone might want to participate in some chat room where it's a closed group, and there might be some degree of testing or something that people want to apply to the folks that participate in it, but nobody needs to know and nobody really wants their real name to be used.

So we might have a digital signature or some kind of authentication technology that would be used deliberately anonymously, but to apply to different people. And then it would be totally different and we would want a completely different authentication technology and probably I might prefer this biometric technology that would allow me, this Margo Saunders, to buy land in Montana so that any other Margo Saunders -- and actually I have searched the net, and there isn't any other Margo Saunders on the internet.

And that's why we don't want a national ID. We don't want one authentication technology. We want a whole series of them. And issues is: A, how reliable they are, and B, who holds the purse strings if they

are proved wrong?

MR. ELLISON: I actually met someone who provides an example of that chat room that you're talking about, your hypothetical chat room. He runs an on-line discussion group for incest survivors, and two of the characteristics of this discussion group have to be first of all complete anonymity because an incest survivor is so sensitive, so fragile, that this person will not open up and discuss it except under strong anonymity. But you also have to have very strong access control. You have to know that only fellow incest survivors have access to this group for

dealing with the off-line world merchants that I think I've been dealing with or even on-line world merchants that I've dealt with in the past.

MR. TORRES: I think absolutely. I was just thinking fully it's a two-way street and I think sometimes the consumer advocates and the industry folks who have created this sometimes wonderful technology above each other, but it really is a two-way street in the same way that businesses and the service providers want to authenticate who they're dealing with, consumers need to know -- and I think it's even moving beyond just what the OECD and other people have about, you know, getting a name and address, a way to contact the business with a proper telephone number, but also to truly authenticate who the other party is that you're dealing with on-line, and in the same way you're talking certifying or authorities for consumers, it's almost as though we need the consumer thing for the business.

MR. MEDINE: Sure. Mike.

MR. BAUM: Sure. And as it turns out, for example, our company, Verisign, has issued about 1,250-plus certificates to businesses to authenticate their web sites, and we haven't seen any litigation yet; and it seems to be working. And while, of course,

we can get into a thrash of precisely how we should identify that person or what type of name structure we should use, it seems to work.

You'll remember an interesting thing Carl said a little while ago. He said, quote, there is no PKI.

Well, while certificates have not been widely deployed for end-user consumers as of yet, from the perspective of certificates issued by certification authorities within globally deployed PKI, that's out there, and what is interesting is if you think about the number of actualness instances in which these certificates or actually being used at this moment, each of those certificates of every web site, so for example, every time money is sent for example over Amazon.com or for that matter some of the transactions at Ebay or wherever else, the certificate is being used to authenticate the web site to the user and to assure a secure communication channel. That's not digital signatures from the end-user consumer to the company, but it certainly is an authentication mechanism. It certainly is part of the broader global PKI that's already been deployed, and it certainly has been of great value to the enhancement of electronic commerce generally.

MR. ELLISON: And yes, thanks for correcting,

Michael. I was a little sloppy when I said there is no PKI. There is this existing set of certificates issued to merchants for SSL purposes, and the browsers do check those certificates.

I do have a complaint with the browsers, and that is that the information that they check and verify is not provided to the viewer. It's made available on an option, but I don't know of anybody except me who actually goes and looks. But that's not the point I wanted to make.

David, you said that if someone might have gotten a domain name for that well known name, IBM.dot. They didn't get that name or they didn't get Intel.com. For well known names, that's fine. These are names that all of us agree on.

I assume everybody in this room would agree that when I said Intel, you think of the same thing I think of, but I don't think that's the issue with electronic commerce and especially not global electronic commerce. I think the issue is that we are running into web sites we have never heard of.

You've never heard of this merchant. You will never encounter this merchant physically, somebody over -- Dorkmund, Germany, you're not going to run into them on the way out of the door of this building. The

question I think we need to answer, and this was addressed some in this morning's session, what happens when you move to a new neighborhood, and you have to decide what dry cleaner to use or where to do your food shopping, what drug store to use.

You can go into a store and look around and see how well kept it is, how efficient it seems to be. You can talk to some of the sales personnel in the store, or you can do what I do, which is talk to my neighbors. I said, by the way, what is your dry cleaner? Do you have a favorite doctor? I get recommendations from people. That's the mechanism that I believe we need the most, not just a mechanism that securely attaches the real name of this merchant to his web page. That's the mechanism that is proceeded today by SSR certificates, but if I never knew that name, if Hanz's Bakery in Dorkmund is unknown to me, the fact that this web site came from Hanz's web site in Dorkmund doesn't help me. What I want to know is how good is their product. How good is their return policy? Do they ever cheat their customers? That's the information I need to know, and that's not being provided here.

MR. MEDINE: And stay tuned for tomorrow's discussion in the afternoon on seal programs as

potentially a start in that direction.

Mark, do you have a comment?

MR. BOHANNON: I was just going to --

MR. MEDINE: Can I just introduce you as Mark Bohannon, who is the chief counsel for technology at the Department of Commerce and just -- as you know from this morning, has been very cooperative in helping us put together this workshop.

MR. BOHANNON: I was just going to -- Carl sort of jumped the gun, but I mean underneath the rhetoric around the WIPO process to speed resolution is the next very serious question that Carl raised in making sure that you have confidence in who you're dealing with, whether that's the owning of the domain name or the web site or anything else.

I also think it raises a question that has not

It was the two of you working together with us and with NSI that shut them down, made them pay a fine, and as an example, I think, of the kind of cooperation we're trying to get here.

MR. MEDINE: That's a nice transition into talking about the international workshop ramifications of authentication, which is, of course, what the workshop is about. I was wondering if you could talk briefly about where we are internationally in terms of setting standards about what the laws are for both PKI and other technologies.

MR. BOHANNON: Again, this workshop is somewhat about international aspect, so I think I was brought here as probably one of the few people here who were working on this in an international context. Let me preface my review with a couple of caveats and observations.

Certainly I think it's clear from the presentations today that both domestically and internationally when you talk about electronic commerce and transactions, consumers are a key part, but the reality it that what we have dominating right now is business to business transactions.

Naturally, that is therefore the dominant discussion that is going on internationally.

Let me tell you how I think prevalent business to business are. And it's an anecdote going back to the discussions I was a part of almost a year ago when the internet was trying to put together what it believed would be internationally accepted principals for government action on things like electronic signatures. And we got into this discussion about consumer activity on the internet versus business to business, and so I finally just asked, and these were people who are in the middle of engaging in this internationally, what percentage of transactions and what percent of business do you think on the internet is being done on a business-to-business basis to consumer.

Let me say that I was the conservative in the room when I said 85 percent of all transactions. And I think it was important to keep in mind that the fact that most of us in this room deal with the internet in that context of what you like to get off a web site, that really is right now a very small part of what is going on in the internet. So that when you're talking about rules, when you're talking about electronic authentication, you have to make sure that you're fully aware of the picture.

There are a number of developments, and really

my goal here is just to provide you a summary of what I believe is going on, but I think there is, in fact -- I think you could divide the world into two different spheres about how they are approaching the idea of electronic authentication. And it really comes down to whether a particular jurisdiction or a particular forum is operating under what I would call the old assumptions of the internet or I think the reality of the internet.

The old assumptions in my view boil down to the longstanding view that we were going to be dealing with stranger-to-stranger transactions in primarily open systems where we needed hierarchies and digital signatures, that there were going to be very specific business models in which this was going to be done. And there needed to be a focus on the role of this signature of the transaction to enable global electronic commerce.

I think as the discussions here -- as I pointed out, the reality is, in fact, very, very different than those assumptions. That in fact what we have dominating right now are commercial transactions between commercial players that operated in either technically closed operations or as Michael pointed out in a graduation of closed systems based upon private

sector arrangements, whether those be by contract or operating rules or other business practice. And then, in fact, rather than a small number of business models,

So with that in mind, let me try to describe what I see as sort of in a commercial context the two words that are dividing. I would say one-half of the world represented, I think, by the United States, by all Australia, by the United Kingdom, to some degree by Japan, is really a very basic approach that says we don't need to establish rules that guarantee a particular standard or approach to electronic authentication, rather we need to look at our legal framework and make sure that if you do business electronically, it is not discriminated against.

The activities that are engaged here are basically based on the work of a group called the United Nations Commission on International Trade Law, which in 1996 produced a model law on electronic commerce. It is focused on commercial transactions, but with all its work, it could eventually be applied in other areas, but the focus has been on commercial transactions.

So in the United States we have activities like the effort by the National Conference for Commissioners of Uniform State Law to develop something called the Uniform Commerce Transactions Act, which is basically saying don't discriminate i

requirements which say that a record has to be in written form or that a signature has to be in a written form.

The second model -- and again, these are rough; I'm just trying to give you an outline -- says that you need the government to establish the rules of the road, identify the standards, and in some cases create certain presumptions for how electronic authentication ought to be done. And with due respect to people I know in the room, I think the classic model for this is the European Union Signature Directive that is currently underway and more specifically in the German Digital Signature Law, which has been in effect. And both of these say that it is the fold of government to look at the standards, look at the basis on which you accredit certificate authorities. In some cases that gives a heightened presumption to the legal effect of your transaction.

There might be places where the role of private sector arrangements is respected, but it is not, I would dare say, at the forefront of the concern. I think the challenge that we have, and I can say this both as my experience working both domestically and internationally, is that the systems are not going to change how they unfold.

I think the United States is going to proceed as we are. I think that the many of the states in the European Union are going to proceed as we are. I think the challenge is trying to figure out how we make these systems, how we build bridges between these systems. I say that in the sense that it's going to be very important in order to facilitate electronic commerce that we have a common understanding of the goals, the purposes, and the objectives of the systems.

And I think that what we're going to quickly see unfold is, in fact, that many of the differences are not per se about the technological implementations. That there are, of course, always domestic concerns about that, but that there are very different approaches if you are a common law country versus a civil law country. If you have a culture in which the government has for many decades in some cases centuries played a central role to making commercial transactions or other kinds of transactions valid, that at some level it's not about the electronic authentication that is going to be the most difficult part. It is looking at what are longstanding cultural and legal systems to see how we can make them work more effectively together given the global nature of the economy.

So with that I give you that overview, and to

emphasize that again most of what is going on internationally right now is commercial, but consumers do come into contact since consumers often rely on those commercial parties in facilitating their transactions abroad. Lord knows the last time I was in Paris I was very lucky that a certain company's network worked and that the contract between the merchant bank that I was getting the money from worked and that the system worked. So consumers are relevant, very relevant to this discussion, but the international issue right now I think is being focused on is the commercial nature of these transactions.

MR. MEDINE: Thank you, Mark, for that summary.

Margo, in your paper that you submitted, you talked about an alternative to dealing with existing infrastructures, which is the creation of a world consumer organization. How do you see that playing into setting the rules for authentication?

MS. SAUNDERS: There are a lot of other things I wanted to say. Can I say those things and then answer the question?

MR. MEDINE: Sure.

MS. SAUNDERS: I'll try to be brief. I think there's very different -- there's quite obviously a very

diverse set of opinions here at this table, and I think I would like to pose a question that you have not asked and answer it. I a few of us, Frank and I particularly, are very interested that you hear this point on this issue.

The development of the Uniform Electronic Transactions Act, which my friend from the Department of Commerce has referred to, and similar laws on the state level, has established a -- have been -- have gone on with the basis of -- with the basis that most transactions entered into between parties on the internet are truly negotiable by both parties and that both parties have equal bargaining power and equal access to information and equal access to choices. And that is certainly true in many situations in commerce.

The problem is that when you apply that basic assumption to business versus consumer, now the beauty of the internet is that presumably it opens up the marketplace for all consumers and allows consumers to shop or realistically much more broadly for whatever it is that they're looking for. But the fact of the matter is that every consumer in almost all situations are not allowed to negotiate the terms of those contracts with those businesses, and either they take it or leave it.

There are adhesion contracts which they cannot negotiate, so that when for example a large business says you shall use this digital signature, this digital certificate, this certification authority in order to transact business with us, and we will rely on the private key or the public key issue, the private key technology provided by this certifications authority when we accept your orders to make checks, have checks written to someone else by land or whatever it is that reg Z doesn't apply to, the consumer has to accept that those rules or not do that, not do this. And the consumer, most consumers in this country at least transact business with most businesses with the understanding that there are basic consumer protection laws that stop unfair and deceptive and just plain wrong behaviors, and generally there are. They're state laws and federal law. There's generally federal laws that prohibit that.

But what that means is that the lawyers that Mark was referring to, you're assuming that those laws, the electronic, state laws assume equal party distinction between the people bargaining, and that's wrong. And that means the consumers are going to be left holding the bag when that certification authority has made a mistake and has issued the certification for

this particular transaction which isn't valid.

MR. BOHANNON: I want to make sure we are talking about the same thing, because I want to make sure that, you heard me say when I was talking about the Uniform Transaction Actions Act, I clearly -- this administration and I will be absolutely clear, is making absolutely no judgment about the Uniform Computer Information Transactions Act, which I think you were describing, which comes out of the disaster of a disaster clearly.

So since we are almost in agreement, but I want to be very clear that what I was describing it was not USIDA (phonetic) it is the Uniform Electronic Transactions Act, which the authors have meant to say as in many of these cases is primarily about commercial volume transactions and really deals with a very, very simple proposition to enable electronic commerce.

It's not talking about the validity of the contract, USIDA does. It's saying that putting the validity question aside, making sure that there are not written requirements that are discriminated against to enable electronic transactions. It doesn't go to the validity question at all. So I just want to make sure that there is no confusion of what we are talking about.

MR. MEDINE: I guess the question is should there be a different set of rules for business-to-business transactions where businesses can negotiate at arm's length and set the terms, as opposed to consumer-to-business transactions where consumers typically don't get to negotiate those, and if that's

as much as business-to-business transactions have occurred or because it's so new and people are just getting into it, we really shouldn't have any regulation, where at the same time it seems that like that's always the case or self-regulation when it comes to consumer concerns. But when businesses have a concern, I'm certain that we've seen a full slate of proposed legislation. You saw the UUCC2B that has been turned into this other monster come up. So it's just a bit unassuming when you say any regulation is a bad regulation. I don't think that's the case at all. I think that in order for consumers to have confidence in the internet, they need to be assured that some basic elements are there.

If in the best of all worlds, it would be great if we could rely on businesses to take it upon themselves to say, look, we'll protect your privacy or we will give you control over it. We will assure that our site is secure, so that the information you provide won't get into the hands of somebody who will use it to take your identity.

We have -- to the extent that you are purchasing a product from us, you will know what our return policy is. You will know what it costs to deliver it. Unfortunately, that's not happening. And

so, to the extent that it is, if I were -- I'm not in business. If I were in business, I would say, fine. Put in the protections, because I can adhere to that. We don't want cumbersome, burdensome things. We're not asking for that. But to me that helps the bakery in Dusseldorf or whatever to actually compete with the bigger players on the web, because the rules are the same, and the consumer can say I can buy that pastry and have it shipped to me overnight knowing that there are some protections in place for me, that I don't have to rely simply on the brand names that I feel comfortable with.

Because if you're solely relying on the brand names that you feel comfortable with, then the internet becomes kind of this novelty it's great to kind of surf and get all this great information from, but to really make E-commerce work, if you're just going to the big brand names, is it really beneficial to you? Are you really able to shop for the best price? And so that's where the whole notion of having another system come into play, because we are talking about a multitude of jurisdictions. We are talking about a lot of crossorder transactions with this thing. It's going to work the way everybody says it is.

So the only thing that it -- I hate the expression we have got to start thinking out of the

box, but if there's ever a time to do it, it's now because the benefits are just tremendous from this technology, absolutely tremendous, but everybody needs to be good actors. We'll always have fraud. We'll have bad actors. We'll have bad businesses. We'll have consumers taking advantage of the system, but for the people that really want to use it, let's set up a system that benefits everyone.

MR. BAUM: I can agree so far as the notion that, yeah, we need to start to think about this today. Anyone that knows me probably knows I've been thinking about it a long time, so I applaud that. And we should be here today, and we should be engaged in precisely this discussion. Having said that, I've got tremendous concern about a knee-jerk reaction in this area.

First, we're not, at least in this panel at least, I believe, talking about general consumer protection on the web. Critical issue. Other panels at this meeting. I thought we were here on the authentication piece. So in terms of general consumer protection, good practices and resolving many of the type of, you know, nightmares that we heard upstairs, my viewpoint on that is a separate issue than where I want to go right now. On the authentication piece, I think we really need to work with the following points.

The first one is notwithstanding at least the hypothetical, if not on a practical level, the potential harm that could come up with some scenarios, I haven't seen as we've seen in congressional testimony, the panel of victims. I don't see it yet, and if it's not there, what's this notion about short-term regulations?

Second point, the vast majority of the transactions I've seen, and perhaps it's growing and maybe Russ has something to say about it, is there are being down with credit cards on the net. So you've already got at least some of the better consumer protection laws in place. This is nothing new.

So if that's the case and if that's the vast majority of commerce, then what are we talking about in terms of the regulations of authentication at this early point when you're hearing about the biometrics industry just starting up, the PKI industry just starting up and other technologies and getting started here.

Let's go beyond that. If you look at the uniform electronic or strike that -- at least the Bliley (phonetic) bill that I think I saw, there's something out there in that regard, family law transactions.

So one of the big problems we've seen, and I'm sure the statute of frauds would cover chunks of this anyway, is the short-term concern of the grandma losing her house or her estate, may not be much more than a sound bite at this point.

So let's really even go beyond that, since we already opted out of the exception of the credit cards and everything else that I, mentioned. So now we are down to probably one of the killer applications that we're going to see out there in terms of the broad scale use, and it's really -- it was late in coming, and the industry can be criticized for that. Others can be criticized, but it is secure electronic mail.

So the extent that that's really going to be the fantastic application to provide really hard-core privacy between consumers with regard to their personal confidential communications, including the communication of credit card numbers, thank you very much.

In that regard, again that goes back to the type of model that I presented up there, this nontransactional model, this is just direct communications between two parties once they have some types of authentication technology to use. And, of course, PKI is a good one.

In any event in those types of transactions we're not involved in, that's not even part of the authentication per se.

Now, certainly you'd want to identify the party on the other end, but even then, if you think about what Carl mentioned about a group of -- what kinds of survivors?

MR. ELLISON: That was incest survivors.

MR. BAUM: Incest. In that case, you may not really care so much that the given person is a member of that particular group, as you care that over the course of time that you're communicating with members of that group, that you're dealing with the same person. So the notion of the importance of being able to have assurances of the sequentiality of communications may turn out to be a tremendously valuable capability.

So where am I going? I'm trying to suggest that the scope of applications, and by the way that latter half didn't involve any money at all, by the way. Of course, privacy and health information are critical. The notion that I'm trying to raise is we're just getting started here, folks. And the nature of the actual risk, I think in actual terms of actual use, may be different than what some people in this panel

are making it up to be today.

That doesn't mean we don't take seriously what you're saying, but what it does mean is maybe the following: We listen just as we are engaging, but I truly believe for any type of viable authentication laws have to come out that are going to be broadly based, get uptake internationally, and, boy, don't we know how important it is that we don't act alone here in terms of having the scope of international capability, but that's probably going to take a few years of work. But to the extent again we don't see the victims today, I strongly urge that we don't have a knee-jerk reaction here, but we methodically put good resources into thinking this thing out and really take advantage of the international forums that have already given this a lot of thought.

MR. SCHRADER: I was a little bit concerned about the international dimension and since it was raised, I just want to address it.

I'm not sure that there is in any way an agreement as to what international consumer protection should look like. Example, the one that is traditionally used is in France, they use a seven-day cooling off period. In this country, I send to

Amazon.com, I want that book now. Tomorrow is too late. I don't want it in seven days. You think about sending it, Lord knows what kind of stale bakery I wold get from Germany.

In terms of the consequences, when you take that in, I will submit it would be extraordinarily difficult for a new business like Amazon.com to even exist under that kind of a law.

The competitors where you can get your book down the street and any place else that was not subject to that kind of handling that was done in the name of the consumer protection would stifle some of the unique opportunities that has started to reform.

Once again, we talked a little bit about contracts of adhesion, the take it or leave it aspect of it. I don't know that it's any different where I'm in a small town, and there's Walmart, and there's a small hardware store. At this point in the internet, I can tell them take it or leave it there and go to 27 different purveyors of CDs and tell them I'm going to leave it because the 27th one has a little bit more competitive advantage. That's where the competition that we are trying to encourage comes from.

I think the private sector working through the credit cards, that's tomorrow. I just want to talk a

little bit about the internet.

MR. BOHANNON: As I said, my expertise is more in the commercial law area, but I hate to pick up France again, but it's fun. For example, this is a serious question that we are trying to address about how to ensure effective confidence by consumers in international transactions. For example, what do you do with a situation where in France the fundamental difference is even more than you talk about. In France, there is nonrecourse banking. Well, there is in the United States. In France -- well, I would say most people in this room have a credit card issued by a bank that is not where they do their traditional banking. My guess, most of the people.

In France that's not the case. It is you get your card issued by the bank you do business with. That's affected the ability of many consumers in those countries to be able to use the same rights that consumers have here to say, look, I want to put a 60-day hold. I want to have this investigated.

The question is not just about what you do with a piece of plastic, and the rights that are a associated with that. What we have are very significant different traditions by which a variety of consumers rights. And I agree we've got to figure out

some way to make it more transparent, to make it more open, to understand how businesses can do.

I just have to wonder whether we will be sitting here a hundred years from now with the same panel with David and having the same discussion if we try to talk about truly harmonizing consumer laws as opposed to having them work in harmony. That's an important distinction.

MR. BAUM: And I don't think either Margo or I were implying that we should adopt the laws of France. But at the same time, there is a lot of discussion going on at the international level. I'm talking about consumer protection and discussing things like authentication, digital signatures, and how they apply in the consumer's realm. I think they are important. But, you know, we're not talking about adopting the laws of France here.

MR. MEDINE: We have time for just a couple of comments.

MR. ELLISON: Yeah. Michael reminded me of just a couple more things that I like to point out. I tend to think of transactions over the web being all by credit card as Michael suggested, but they're not. Intel does a huge amount of web transactions business to business, and it's not by credit card. It's by

purchase order.

When I was back at Cybercash, we were worried very much about how do we do electronic checking. That's not credit card protected. Electronic use of ATM cards unless the ATM card happens to have a Visa logo is not credit card protected.

So it's not just credit cards. It would be nice if it were in a sense. A little myth Michael. I couldn't resist it. The secure electronic mail is not that new. Anyone who has got my business card has my got my PGP fingerprint. And that's been around since 1991. But the serious point is that I believe I agree with Michael. We are here to talk about authentication, but what's important to me is not to use this authentication for the purpose of identification, attaching a name or some other ID to a key holder, because that assumes that I know how to make use of that ID. You know, if I have somebody's social security number attached to a key, heaven forbid, that assumes that I know how to use that number to look something up that is of interest to me. What is important to me is that we have the

signed into this certificate, attached to this key holder by somebody who is trustily an authority on those attributes.

If the attribute is my permission to use the credit card because I've got a set card holder's certificate, that certificate was issued by the issuing bank. That's the true authority on this piece of information. So I've identified a piece of information I need to know about that key holder, namely permission to use that credit card, and I've identified the true authority for that kind of information, the issuing bank.

Sure enough this piece of information comes to me issued by that true authority. That's a wonderful example. I worry about us not paying -- the people who did SET spent a lot of time asking themselves what is the important information and who is the proper authority to issue this information.

What I worry is that we don't do that in other things that we need to know. I worry when people talk about authentication is just attaching an ID of some form to a key and assuming, well, now we've done that. We can go deal with other stuff, because that's not the issue.

The ID is almost always useless because the

world is so big. We need to know what it is we want to know about a key holder, and then for each of those things we need to identify who is the authority.

MR. MEDINE: Margo, last comments.

MS. SAUNDERS: Michael is very worried that, I assume, that the FTC is going to come out with a recommendation that digital signatures and PKI technology be regulated immediately by Congress. Right?

I would not be at all dissatisfied if they came out with that, although I would be very surprised.

I think where I am going, and I expect other consumer advocates are going with this is that when there is an independent certification authority that a digital signature or some authentication technology serves -- is to serve a particular purpose, whether it is that I am Margo Saunders or that I am an appropriate member of a particular chat room, anonymous as that may be, or that I have the authority which may be from my husband or from a friend or from a corporation, to use a particular credit card, whatever the purpose is, if the certification authority says that I am that person with that authority, the question is, what is the liability that attaches to the certification authority if I am not that person, and if I have access and am

able to use that authentication technology inappropriately?

And that's the regulatory question that I think we need to answer. I envision a multiplicity of authentication technologies for a huge variety of reasons, because the last thing we're going to get in this country, I hope, is a national ID.

We want for some transactions the anonymity that the internet offers us, but we need somebody to enforce, if it's not voluntarily enforced, the promises that are made by the certification authorities, whatever they are, and to hold the certification authorities liable when those promises are not kept. And individuals that and potentially businesses suffer as a result. And that's the regulatory, at least, path that I think we should be investigating.

MR. MEDINE: Thank your for provoking a lot of good questions, and as with other subjects in this two-day workshop, we do this as the beginning of the debate and the discussions and not the end of it. And I would like to thank you, all the panelists, for their tremendous contributions. Thank you.

(At 4:52 p.m., the proceedings in the above-entitled matter were concluded.)

C E R T I F I C A T I O N O F R E P O R T E R

DOCKET/FILE NUMBER: P994312

CASE TITLE: Global-E Marketplace

HEARING DATE: June 8, 1999

I HEREBY CERTIFY that the transcript contained herein is a full and accurate transcript of the notes taken by me at the hearing on the above cause before the FEDERAL TRADE COMMISSION to the best of my knowledge and belief.

DATED: June 21, 1999

_____

LAUREL ALLEN

C E R T F I C A T I O N O F P R O O F R E A D E R

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and format.

_____

SARA J. VANCE