World Bank in trying to create a castle in cyberspace and understanding and appreciating the modus operandi of organized criminals as they hack their way into financial institutions.

The modern day state of play in cyberspace is very much akin to Chicago in the 1920s. The speakeasies of today are Internet relay chat rooms where personal identifying information is being sold at whim as well as access to owned systems. Owned systems being systems that have been compromised by criminal groups and/or networks

Modern imaginary lines are not sufficient in protecting us in today's day and age. Firewalls are acting like moats around castles. They can be penetrated by the various ports and applications running through them. PKI is only as secure as the private key and the certificate authority. And last but not least, intrusion detection systems need to be tested and actually war gamed to essentially understand how they might react in battle.

Preferred tactics of hackers. What's most interesting of these is the reality they're already inside of you. They are probably already inside your corporate network attacking you from the inside out. The myth of the insider threat being the greatest threat is highly problematic because in reality it's much easier to buy an owned system or compromise a system inside a network perimeter than it is to have a user inside sitting at a desk going through the whole rigmarole of being an employee. As you can see phishing has exploded. To that note one of the biggest things is data warehousing companies and web hosting have become a real Achilles heel in our network posture. Hosting companies themselves with only service level agreements are becoming a focal point of attack. A bull's eye's in the sky for organized criminal syndicates. If I want to hack into 300 banks, I'll go after a bank hosting company. If I want to hack into 20 government agencies, I'll go after a major data warehouser who does business continuity services for the federal government. I don't need to attack each one individually anymore. And most of these hosting companies don't have proper security in place.

Pharming is a huge problem. We keep talking about phishing and how it's the user's fault. The real problem here is that web servers can be compromised, DNS servers can be compromised. Users can go traverse a website and get Trojan horses shoved down their throats. This is reality. This has grown 5,000 percent since last year according to a SOFO study. We need to recognize that proper webserver security, proper due diligence in maintaining the sanctity and security of our websites and DNS servers will slow this trend but not stop it. We need to start focusing on other things than user ignorance.

The key problem is root kits. No matter how they're getting inside of you whether they're attacking the hosting company or whether they're attacking web servers, they're installing root kits. Most of these things are unidentifiable. Most of these things have multiple capabilities, they maximize their intrusiveness, in terms of clandestine hiding their position and allowing them to covertly attack your system at whim. Most of these root kits are being highly programized in the sense that they are targeted in nature. They are only being distributed to one or two or three targets. They lie in wait for various financial transactions and/or other sensitive data to be accessed. A recent Symantec study demonstrated there is 600 percent of use of these in the wild last year.

Authentication. We really need to get down to two-factor authentication, not multifactor authentication. The criminals have already gone down this route. The modern day Trojan horse is not a keystroke logger, it's a session-based Trojan which takes screen shots of everything that you're doing on your PC. So if you're picking an image, you're not defeating it. You're not defeating anything. And the reality is they've built out these Trojan horses now to do screen shots versus key stroke logging because they're more aware than we are of our defensive response.

How can we stop phishing? How can we stop any of these things? Let's just talk about phishing. How can we really stop it? Give users real two-factor authentication, which is something you are, something you have or something you know. Use toolbars to identify malicious webpages. Educate consumers that you'll never send them an email asking them for information. Educate consumers how to identify a spoofed email. It's simple, it's R squared: if the reply path and the return to is not the same thing, you have a fake email from a fake entity. Teach them how to read headers. This is important for all of us. Change the mother's maiden name to a different password on every one of your financial accounts that way when they finally do breach that financial database, they won't have the right information to set up a line of credit. And penetration test your web servers and email servers on a quarterly basis to determine where they're vulnerable and how so that pharming attacks don't proliferate through your customer base. Last but not least, mandate remediation time tables for these tests. We can't just test and say we found these holes, but we're not going to spend the time and money necessary to harden the services. Lastly, I really believe in this. Why should we not be allowed to initiate credit freezes if we don't think we want another line of credit this coming year? Thank you.

>> BJØRN SKJELBRED

Good afternoon. Thank you for inviting me to this workshop. It is very useful to us to share some of our experiences and to learn from others what they're thinking and planning.

I'm representing a Norwegian bank. We have some experiences in how to implement the different technologies as was stated. So I'll share some of these thoughts with you.

The main choices that I see just now are and will always be usability versus security. The more secure the solutions, the more cumbersome and the less use you will have probably. So this is a balance you have to find out for the whole future, as well.

Right now we do see new user habits and demands as well which will challenge the technologies. I want to say something about that. And see the new kind of global growth in business which will control how to meet these kinds of threats.

The customer demands regarding online banking services will of course be any time, any place, anywhere. Ease of use, no user manuals and so on. Very few things to remember and rather no extra items to carry around in your pockets or in your bags.

The problem is that we have to use some kind of technology that requires these things to carry on and so on, to try to >>Bsy a-threatssnill.sitTd[p0.0016 Tw 17.355 0 Tdujoe[p0.0016 Tw 1o)8(T185)u2

And also moving from only using PCs in an open network to starting to use mobile phones, PDAs and even TVs to access our online services is also a challenge for the technology, which is mostly based on PCs and servic have been compromised. And what I find is people -- and you can argue that our customers are even the most cautious or the most paranoid, take your pick, but they are people that are actively managing their identities and trying to make sure that bad things don't happen to them. And what I find, and particularly people who have either been compromised or who are in a risky situation – either they travel a lot, they're going through a divorce, there's something going on that heightens their awareness. And they'll ask us to put on additional identifiers on the account. So beyond what we ask for, beyond the things that we do, they'll ask for additional items put in there because they know they're at risk. And so we're seeing this. And it's very interesting. And again our consumers may be more savvy than most customers you see today, but I think it is an interesting trend that people will take the time to do that if it's convenient and if it's secure to

So the framework works across -- the thing that would be great is if businesses got together not only to share what happens with good identities but also to share the bad actors, whether they be real bad actors or whether they be synthesized bad actors. There's no way somebody is coming into me and I can go against a database of bad actors to see if that person's there today. That would be nice to have.

So we don't have all the answers. But we're trying hard. And again we're trying to stay ahead of the fraudsters and the other bad guys out there. And trying

don’t get a lot of joy out of fiddling with it and installing new software and hardware, this is the perfect thing.

So that’s what we’ve seen again in the consumer space.

In the corporate space, the solution that seems to have the most traction is basically the one time token password-generating tokens. You’ve heard from some of those vendors today. There are a variety of manufacturers. Basically this is the little key fob that generates the new password every 30 or 60 seconds.

Now in the consumer space, that has not gained as much traction because it is more expensive. In other words, the bank has to pay to give each customer one of these tokens. And there’s more administrative cost behind it. You have to set it up, make sure it’s running. So it makes more sense I think for banks to do that in the corporate space where the cost differential is not such a big problem.

One thing I would also say is that regardless of the space or regardless of the technology, what we have seen is that almost every bank -- I think virtually every bank I’ve seen is basically using a layered approach, which is they are not relying on one technology or one technique and one technique only to authenticate customers. And from the banking regulators’ point of view, that’s a very good thing because no -- as we’ve heard many times today -- no security solution is perfect. And the idea of putting more locks on the door means that your solution is ultimately more robust.

So what we’ve seen is say if you’re in the consumer space and you have device authentication as your primary method, the first thing the bank has to do is figure out well if that method goes down, what am I going to do? Because in most cases I do not want the default position to be, if I’m a bank, to deny my customer access to the website because that’s not good business. So most of them, from what we’ve seen, have used some sort of challenge response, basically knowledge-based authentication to say if the device authentication fails, we will ask you a bunch of questions and see if you can answer them because we really want you to be able to get into the website and do your business. And that seems to be sort of the basically the fail safe force if the primary method of authentication doesn’t function for whatever reason.

Well, what we’ve also seen is that banks for the most part on the back end now are also running some sort of anomaly detection, fraud detection software to say: even if the customer gets in and they properly authenticate themselves, the bank is going to monitor the transactions. And you’ve heard about this today from some of the vendors and they basically look for and flag anomalous transactions, things that don’t make sense. Especially when money is going out the door and say we’re going to stop that transaction. And either we’re going to stop it cold or we’re then going to, for example, contact the customer through some other band. We’re going to call them on their cell phone. We’re going to call them at home. We’re going to do something to make sure that Jeff Kopchik really wants to transfer $5,000 to Hong Kong when he’s never done that in the five years that he’s been a customer of our bank.

So we did end up with a technology very similar to what Jeff just described, and it was basically a pattern adaptive type of authentication that we added to the log-in of our website. We have about 50 million card members. And our website's discovercard.com so it's one of the top 100 websites that gets quite a bit of traffic. And when we thought through what we wanted to do primarily among our concerns were what he had mentioned: would people stop using our website? And the cost involved with that. So those two things taken into consideration were how we ended up with the techno with really two things. One was the communication and how the information was communicated and the other piece was not having it sort of one day flipping a switch and now suddenly everyone had to do it.

So those were the two things that we really thought through when we did our implementation plan.

So from a communication perspective, we wanted to try and demonstrate that this was beneficial. So much so that the consumers would be actually interested in adopting it and participating in it and viewing it as something that would help them. And then that message was really around the fact that we were enhancing what existed in terms of using a password. We weren't telling them to no longer use the user name and password. We were simply, as Jeff was saying, adding a layer to that and really trying to make the user name and password an integral part of a layered approach. It's one more lock on the door, so to speak.

And then the instructions for this had to be very clear. So I think the part where I will depart a little bit from Jeff was when he said, oh you just have to have people walk through a process where they select, in our case, three questions and provide three answers and submit that information to us and then they'll never have to really think about it again. For the most part, that's true. The things that we'd run into is that it's not quite that st relatively smoothly based upon the number of customers we're trying to put through it. We are continuing to monitor the call center volume, the web usage at this point looking for the next thing, knowing as all the panelists have said, the technology doesn't stay the same, the trends don't stay the same. Thanks.

>>DICK POWELL

Sorry. I have to go back a ways. Ah, amazing. Didn't have to go back as far as I thought. Hi. My name is Dick Powell, I'm very, very pleased to be here with you this afternoon. Just a few opening remarks, by now, having spent the day here, I'm sure you know that I'm probably not going to tell you anything or share with you anything that hasn't been said by other people already. There seems to be a remarkable convergence of experience and insights here. And that's encouraging to me.

I was asked to focus on the experience our credit union had in rolling out multifactor authentication and how that might be of use to you.

So before I get into that, let me just say that in my lexicon, we don't speak of customers, we speak of members. That's because credit unions are owned by the members and all the employees are members, too. So if you'll forgive me, I'll tend to speak about members. Just in terms of scale, Andrews is a global credit union. We have just under 100,000 members scattered over 150 countries around the world. Including some very nasty places at the moment.

Also I think it's important for you to understand that we approach the rollout of multifactor authentication not as a regulatory issue but as something fully in keeping with our commitment to complete continuous and perfect security for the member information entrusted to our care.

That may sound like motherhood and apple pie. It's not. It's what we believe. And standing in that place, we look at the choices we have to make and the risks we have to manage through the lens of that commitment to our members.

Where's is the advance button? The down key? I guess that won't work. Here we go. Whoops. Okay. Had to go real back.

So first let's just put things in perspective, okay? You've heard this. What you probably don't know is the second bullet, which is in 2006, credit unions led the pack in terms of the percentage increase in phishing. Here's the sort of a little overview slide of that. And it just sort of underscores the problem that the FFIEC guidance and all of the other things we're talking about here today were designed to address.

In the face of this, we chose to take a multipronged approach for our strategy. I want to focus on two particular things, well actually just one. I just need to mention member education and awareness. We have just been talking about it, Cynthia talked about it. Everybody's talked about it. To the extent that your consumers, your members are aware and educated about the risks in cyberspace, they will make intelligent choices. It’s our obligation to help them achieve that enlightenment. And that’s a never ending process.

Sure. Well for us, banking is about trust. The trust is the most important asset that we actually have. If our customers have the feeling that we don’t invest enough to keep the transaction safe enough, well the trust image will suffer from that. That’s a key point. It’s not about the amount of money itself.

compliment one another.

But you have to be careful how you do it because each of these approaches has a privacy component or aspect to it that could be abused or misused, perhaps, in a certain way. And we all have to be conscious of that.

>>TOM KELLERMAN

I would concur. What's most important is that Americans realize that the US Government and corporate America no longer have a monopoly on big brother. And that anyone that knows how to hack or is using an automated penetration testing tool like meta slay can break into most systems and put a Trojan horse there and monitor what you're doing. In order to have privacy, we need better cyber security. There is a disconnect that people profess that if you have more security in a physical world you lose privacy. That may be true but in cyberspace, more privacy can only be gotten and achieved through better cyber security.

Now, one caveat would be I believe in biometrics as part of the solution for two factor authentication but people take shortcuts with biometrics. For example, when they store images or templates on the C drive itself instead of on a smart card. Or they don't have live scans to determine if the biometric is alive at the point of contact, we need to not take shortcuts through the forest when dealing with this scourge.

>>GAIL HILLEBRAND

Thank you. The next question I will ask Chip to lead off and two or more of you to join in. The question is we've talked a lot about how you authenticate an existing customer, how about when it's a brand new customer? Whether it's issuing a new credit card, or an online loan, or something else that's sensitive but you don't have an existing base about that person? Tell us about the extra challenges of open loops.

>>CHIP TSANTES

Again we use similar to knowledge based authentication techniques, all of our customers come to us through virtual channels. In addition, we do some things behind the scenes to look at that person, look at where they're coming from as well to make sure that they are who they say they are. And when we find things that don't fit together, we then channel it to a human investigator to follow-up and make sure it is who they say they are. Not simply technology solutions.

Again, as I pointed out before, part of the problem is that the data is so freely available out there to answer these questions. And these fraudsters are pretty good. They study the questions. They know what's coming up. We have to be on our toes to make sure that we can really spot the -- it's you versus it's someone who has studied you.

>>DICK POWELL

I was nodding my agreement. If a customer walks in and wants to open an account or somebody wants to open a membership, they bring documentation with them. We've heard today about all the problems with even the most valid source documents. That's why all the checks and balances there. That's why all the procedures are in place and why everybody challenges and evaluates. You tend to accept at face value and then validate and authenticate. And if it turns out you've been misled, you take appropriate action.

>>GAIL HILLEBRAND

We heard from, I apologize this question isn't on the list so you haven't seen it before. We heard this morning from some of the bankers about the "know your customer" and the idea that you get a close match but not everything has to match and close the account later if it's wrong. Do you think that's the right standard fo

c (ere pro5.80 from)9(0.08, -or(s)dbnua)85ticT02 T4 09.825 -

because as that dial goes up, I start kicking people out of the system who potentially are legitimate customers. And again from the banking agency's point of view, that's a decision that the institution makes. And then when the examiner goes in and does the exam, that's one of the things, in the big scheme of things, that the examiner will look at. To say well, do we think you put the dial too low? We probably wouldn't complain that it would be too high. But in terms of how did you structure it?

>>DICK POWELL

I would only add that several speakers earlier today spoke about a risk-based framework for making intelligent choices in this space. And I endorse that. I think that's exactly what we're all talking about here.

I also think seeking perfection in an imperfect world is an ex that balance. And, again, I think use multifactors so it's not just the things that they have but it's also things that you're monitoring, as well, to make sure that you're, kind of unbeknownst to them, making sure that their account is protected as they come in. But if I could predict what our customers would do, I'd be in a different business. (Laughter.)

>>TOM KELLERMAN

My perspective is not based on the customer. It's based on the adversary. That being said, the sophistication and organization of organized criminal syndicates as they hack our bank accounts, make work-arounds like we discussed earlier very easy and plausible. For example, if banks are authenticating customers based on IP address, given the reality that root kits and Trojan horses are predominant in the underground and that they're compromising computers left and right, they've already worked around that authentication right there, they've already compromised and botted that PC from which the IP is the only other authentication record. We need to start thinking about work-arounds and how they're going to work around us and have more of a Sun Tzu philosophy on this.

>>GAIL HILLEBRAND

I'd like to start with Bjørn on this next question and then have any of you that would like to add your perspective. Can you tell us one or two things that you are either doing in your company or recommending to be done or you're seeing in your sector that aren't widely done with sensitive information that you think should be done?

>>BJØRN SKJELBRED

Quite a tricky question there.

Well, again, our kind of approach has been to think of continuous development in this. You cannot fix the problem once and for all. So I think that's perhaps the best piece of advice to think that we have to do something now and have to do something new, perhaps in two or three years. And there's still lots of technologies and lots of things to do based on user habits and regional kind of variations. I think you have to try to keep that in mind at least.

>>GAIL HILLEBRAND

Who else wants to go on this question, Jeff?

>>JEFF KOPCHIK

I'll pass on that one.

>>GAIL HILLEBRAND

Okay? Cynthia?

>>CYNTHIA BOHMAN

Well in terms of protecting sensitive data, I think one of the things that we actually do try and do is -- which isn’t so much a procedure within us but to work with law enforcement very closely. Because I think part of what Tom’s bringing up is that you do always have people in organized crime coming up with new various scenarios. And there is some feeling that it’s difficult to find them and difficult to catch them. And it’s just not a high penalty for doing some of these things. And I do think that’s one of the things that we actually have been trying to forge better relationships because a lot of times the data that you would need to truly get those people, part of it resides at the financial institution and part of it resides with law enforcement. It’s not always obvious until you put it all together to build a case. That is something that we’ve always been really focused on, giving law enforcement what they need to build a case. That’s not always something that all financial institutions are in a place to be able to do.

>>GAIL HILLEBRAND

Dick, something that the credit industry is doing right that you think other folks handling money ought to copy?

>>DICK POWELL

I wouldn’t want to suggest that the credit union space is doing anything that anybody else isn’t doing. But one thing we are particularly good at doing is sharing openly with each other. It is something that distinguishes credit unions from many other organizations, and that is that we recognize a commonality here that we share willingly, that we come together in forums throughout the year and openly discuss the challenges we face and how we’ve resolved them or addressed them and openly share approaches that work for us so other people might want to use them themselves.

In a way, that’s what I think this day is all about.

>>GAIL HILLEBRAND

I think that’s right, yes, Chip?

>>CHIP TSANTES

Part of our business is we also help customers respond to data breaches that when they lose data, we provide some of the monitoring services on behalf of those customers. And in seeing that, we get to see sort of the source of these and most of them 8s011 Tw that the credushamm(ghh)6(2( )

week, but again and again updating people. And that’s been very helpful.

>>GAIL HILLEBRAND

Tom, did you want to add anything on this question?

>>TOM KELLERMAN

I think speaking to what Cynthia said, law enforcement is overwhelmed with caseload. I know for a fact because when I worked with the New York Electronic Crimes Task Force and the FBI. They’re overwhelmed. Their central repository for sharing information on this is usually skewed with so many child porn cases they don’t have time to pursue anything else. And beyond that reality, the fact that most organizations are only maintaining their data for one to two months versus the six months that they’re recommending in the EU is problematic. Because when you’re doing investigation, usually it goes back a couple of months and the data logs are gone and deleted because no one wants to maintain that much data. So it’s important that we actually try to hold on to our data longer at the ISP level as well as giving law enforcement more resources and more tracking and tracing capabilities.

>>GAIL HILLEBRAND

Thank you. I know you have questions and you’ve been waiting all day. So -- yes. And there’s a microphone somewhere. It’s coming to you.

>>AUDIENCE MEMBER

So it’s no surprise that people are willing to put up with the inconvenience of authentication if they believe there’s some value in it for them. And most people probably think protecting their own money is a valuable proposition. And so you have some advantage in bestowing stronger authentication on your customer base.

It’s important to generalize and not to mis-generalize from your experience. So the other thing we’ve been talking about today is Real ID. And there are a bunch of people who oppose it because they believe it’s going to somehow infringe on their privacy. So they don’t see a great value proposition in it.

My question is: To what extent do you think having Real ID will help the situation in the financial services community? How will it change the way you do business, if at all?

>>GAIL HILLEBRAND

One of my bankers want to start with that one? Bjørn, I think you’re exempt -- Cynthia?

>>CYNTHIA BOHMAN

I think that from -- I was here just very brie technologists that I've talked to -- now keep in mind, in the banking world, most banks don't do

I'll address this to Mr. Kellerman since he brought this up. You mentioned a second ago regarding ISPs holding data for longer periods of time. How do you address the commensurate privacy risk that comes from that? I'm thinking about the AOL data search query breach. Google and a lot of how their products can oftentimes be construed as being privacy infringing. How do you address that to someone who says "well I don't want these guys holding on to my data for six years." How do you answer that?

>>TOM KELLERMAN

I don't think there is any such thing as privacy on the Internet, first of all. So let's just say I did think that was possible, I would mandate layered security to the utmost on those arrangements. Particularly I think that the banks themselves could have something more than service level agreements like information security service level agreements or secure outsourcing agreements that actually deal with a modicum of auditability and accountability on that process. The fact that banks should be able to conduct a penetration test on the entity that's holding their data and ask for segregation of that data and ask for two-factor authentication on that data. I can keep going.

>>GAIL HILLEBRAND

Thank you. Way in the back. The very, very back.

>>AUDIENCE MEMBER

This question is to Jeff. What happened to those FIs that have not done anything about the guidance? What type of remedies are being required from them? And how is this going to be a deterrent, essentially, for the other FIs to continue to evolve and to implement the guidance specifically around telephone authentication or telephone banking, which is part of the guidance?

>>JEFF KOPCHIK

You want to bring so many this week, so many next week so that you can appropriately respond to the inevitable problems and glitches that are going to occur. An examiner is going to be much more sympathetic to the idea that you went online February 15th because that happened to be your place in the queue. And, again, you were working diligently on it. We understand that there's 8,000 insured depository institutions, not counting credit unions, all of whom who had the same date. So you really have to look at the reasons for it. We are not focusing at the FFIEC level on the latter. If you came online February 15th, you were working on it, there isn't going to be some kind of monetary penalty that's going to be assessed against you. What we're looking to find out are the institutions that either mistakenly decided that they weren't subject to the guidance, and it turns out when the examiner comes in, that they are.

>>AUDIENCE MEMBER

Yeah. How long do you suspect it's going to be before we see an FFIEC 2, given that many of the things that were spoken of by the ge

What we do actually have is one group, our information security group, which is not exactly the IT Czar, but they are a group where all of that information gets rolled up. And they do look across-the-board both from regulation perspective as well as how just, how we're doing from a risk factor authentication and risk mitigation. From that perspective, we also want to make sure that it's consistent. I think our motivation for having that rollup and sort of having one look across the organization is we don't want customers to experience different types of authentication depending on what products they use. We really want to give them something consistent. That is how we do it. I think one of the, sort of, leading points why we do it that way.

>>GAIL HILLEBRAND

Bjørn or Dick would you like to comment on it?

>>BJØRN SKJELBRED

Kind of the same approach since we have several product lines so we likely have the same user feeling. We also have this kind of common security platform on the backbone. And that's important. That they don't have to create different types of security solutions to every new channel you put up.

>>DICK POWELL

I think another consideration you'd want to look at has to do with whether or not -- you may have multiple delivery channels and multiple products, but your underlying application architecture may be unified. You may actually have a service provider or an application of some sort that serves all of those product lines, in which case security architecture becomes just a little easier with that common product.

The other issue I think has to do with what Bjørn just said. You have to have a security architecture for your enterprise. And it has to address technology and process and everything else. And you have to have some sort of a steering committee, if I may, okay, that allows you to bring the stakeholders together and build a consensus. You still have to operate in a risk-based framework. FFIEC guidance calls for that. NCUI guidance calls for that. Payment card industries standards call for that. Everything we've ever seen says the enterprise must do a risk-based assessment. That means there are tradeoffs to be made. And you cannot reach conclusions by yourself. You must have sort of a steering group that brings those stakeholders together.

>>GAIL HILLEBRAND

Thank you. I'm going to take this gentleman in front and then I'm going to ask if your questions are about the FFIEC, please hold it until after the panel.

>>AUDIENCE MEMBER

This is a question for both the financial institutions and the regulators. And it's picking up on what Chip mentioned offhand a little bit earlier.

We're talking here about defending data within the organization. I'd like to ask if it's time to look at Gramm-Leach-Bliley which allows by cleverly wording the annual policy statement to ship lots of data out to the third-party marketers and other entities upon which you have agreements without allowing the customer to even say "I

How would we stop that?

>>CHIP TSANTES

One, you would give consumers control over people acquiring that data so that I would permission the acquisition of that data about me and its uses.

Secondly, if you are someone selling that data, you would look for a reasonable use. It's a reasonable use on ancestry.com that I would look at my ancestors. It's not a reasonable use that I would look at yours. That's crap. But you can do it now. With my account I can do it and I can actually set it up so I can just mine that data even though I'm only supposed to be a single user doing it, and I've done it. It's very easy to do.

>>GAIL HILLEBRAND

Anybody else want to comment on data broker, data mining?

>>AUDIENCE MEMBER

Return to the question posed at the beginning. The first question that was posed in this session was asking about Real ID. But pushing past that, let's posit a system whereby government has intermediated a unique electronic persona for people in the United States or whatever. Which is, to me, not merely an authentication issue but it's an underlying identity issue. How would that positively effect your operations? I think, Chip, you in particular raised that as still an ongoing issue. Could you speak to that and maybe the others of you here, as well?

>>CHIP TSANTES

I'm sorry. Can you repeat that?

>>AUDIENCE MEMBER

The first question posed today was about real ID and what the effect might be. But many of us believe that Real ID is insufficient. If you were handed a government intermediated mechanism whereby there was a unique electronic persona for any one of your potential customers with built-in physical presentation where necessary for triage or other kinds of factors, what are the positive effects upon your business line?

>>CHIP TSANTES

Again, we only get virtual customers. So if I could better trust the credentials that are presented coming in, that gives me a better assurance to release that. Now no matter what I would never rely on one factor, or one mechanism to do that. I would monitor. I would have a multilayered approach because I'm not smarter than the fraudsters. I'm not smarter than the criminals. And as Tom pointed out, it's gone from mischief to a professional activity with very smart people working on this problem full-time. So I’m not going to rely on one thing, especially something coming from the government.

>>GAIL HILLEBRAND

Last question. Yes?

>>AUDIENCE MEMBER

There seems to be a disconnect here in that folks keep saying that folks want privacy and then the statement that follows indicates that people want security. They don’t want money stolen from their bank account. They don’t want to have people take out bogus loans in their name.

The two are not necessarily the same. And there are people, I mean when we started the web, right at the very start of the web, the thing that got folks hooked was publishing information about themselves. When we only had 100 people on the web. There was no Google. There was no where to go. The only use for the web was if you were an extrovert and wanted to describe yourself, wanted to publish information on yourself. And I think that something has to go here. Maybe instead of people describing themselves and sharing their genealogies, maybe what has to go is the financial system that rests on the idea that information that isn’t secret, that is really easy to find is difficult to find. Maybe what we need to do is to go to an idea where if somebody wants to take out a loan in your name, that you have some strong binding and maybe really instant over the web credit of the -- you can borrow $40,000 mortgage with a mouse click. Maybe that’s the thing that has to go.

>>GAIL HILLEBRAND

Tom? I think that one might be for you.

>>TOM KELLERMAN

I think that in the end, that may be the only way we can go. It really may have to come down to that. I mean, all the things that the banks have done in the last five years to improve security, can you now go to the FBI and secret service and say bank fraud has declined? It hasn’t declined yet. It keeps going up. It goes up by hundreds of percents every year. And agents have to pick and choose cases they’re going to proceed. And part of the problems is that PII has become virtual cocaine. There’s no point in selling drugs or human trafficking anymore when you can set up a $100,000 line of credit in your name by hacking one database. The criminal minds themselves don’t need a business model anymore.

>>GAIL HILLEBRAND

On that note I’m going to ask you all to come back tomorrow morning 9 a.m. We’ll be starting. Help me thank the panelists. 8:30, I’m sorry.