TRANSCRIPT

PROOF POSITIVE:
NEW DIRECTIONS FOR ID AUTHENTICATION

PANEL 5

APRIL 23, 2007

>>NAOMI LEFKOVITZ

All right. Why don't we go ahead and get started? Our last panel of the afternoon, but not in any way least. I think you're going to find this to be very interesting. We're going to talk about implementing all the technologies that you just heard about. And our moderator is Gail Hillebrand, she is a senior attorney with Consumer's Union.

>>GAIL HILLEBRAND

Thank you, Naomi. We've heard a lot about technology today. Now we're going to talk about some of the practical questions, some of which we started in the last panel. We're going to talk about how you make the business case within your own company to spend the money on technology that protects not only the company but sometimes other people, like the customers and third parties. We're going to talk about how you train your own employees within a company to accept and work with the technology and to see the protective value that it has. We're going to talk about how you educate, train your customers. And we're going to hear from the FDIC about the role of government. You might say this is the implementation panel. You might say this is the banking panel. We have a lot of folks from financial services industry here. We're going to hear first from Tom Kellerman. Tom is now at Core Security Technologies but previously was involved in risk management for the World Bank, advising central banks about their risk management. Then we'll hear from Bjørn Skjelbred. Bjørn's from DNB Norway one of the largest financial services groups in Norway. The EU seems a little farther along than we are in some of the authentication issues. He's going to talk not just about spending the money but how you keep up-to-date as these technologies change and how you urge your companies to invest and keep them up-to-date. And then we're going to hear from Chip Tsantes from Intersections, a company that develops and markets identity management solutions. And then we will hear from Jeff Kopchik. Jeff's going to talk about the two-factor authentication rule. He's not going to tell you what's in it. You can read it on the website. He's going to talk about some of the practical things that have come up as U.S. financial institutions have tried to implement that rule. Finally we will hear from Cynthia Bohman at Discover about how they're protecting their customers and the other third parties. And from Dick Powell from Andrews Federal Credit Union. Tom?

>>TOM KELLERMAN

Good afternoon. Much of what I'll say today is based upon my experience with the

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. It is important to note that they work in a very organized fashion, these groups, in a very ephemeral sense. They don't meet each other necessarily in person but they have common interests. They sell common attack code, systems access, data mining capabilities and money laundering capabilities at whim. The average sales price for an owned computer in a corporate network today is about 4 cents. That computer is typically called a bot.

Motivation has changed. It used to be narcissistic. It used to be about bragging rights. It used to be about taking down systems and affecting as many people as possible. But today's day and age criminality in organized crime has moved into this space and in doing so they have made the primary attack vector being financially motivated. Banks are the most heavily targeted. Many times you don't hear about it because of reputational risk issues. Then again banks do have a better layered security posture than most E-commerce organizations but in doing so there are certain gaps in security that are noteworthy for all.

According to Gartner, 15 million Americans lost their identities last year. FTC has been raging about over 9 million a year for the last 5 or 6 years, and these are just the people that are reporting that they've lost their identities, these are just the people that have actually tried to buy a car, set up a new credit line or actually check their credit of which only about 1 in 4 people in America do on an annual basis.

Interesting FBI statistics from 2005 as you can see. More importantly here you have the fact that 61 percent of U.S. computers are probably compromised. Two more interesting and noteworthy studies are one was done by Earthlink two years ago where 1.7 million computers were surveyed of their own user population and over 7 back door Trojan horses were identified on one out of three of those computers. Given the reality that modern day virus scanners are only picking up 35 percent of what's out there you can see how the number could climb. An OECD study, the Organization of Economic Cooperation and Development, stated that about 1 in 3 computers globally were compromised with back door Trojans. The point of the matter here is reputation and operational risk has changed. The Congressional research survey study estimates that between 50 and 200 million dollars in losses are sustained to publicly traded companies who have disclosed that they have sustained a cyber breach. This demonstrates the reputational risk for a laissez faire approach to layered security.

You can see here that over 100 million Americans have their personal identifying information jeopardized, or at least it's in the open now. This is according to New York Times and privacy rights clearinghouse based on a number of successful records that have been exfiltrated from networks from the data breaches that have been reported over the last two years. The problem is our defensive posture has been based upon the main frames of yesterday.

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 convince our customers why to use the token, carry it around. That is a problem for us introducing new services.

Regarding changes to what people are doing, they are not only doing online banking anymore. They are reporting to the government and applying for jobs, applying for many things. So we have to meet new kinds of demands that these services really demand of us.

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 services, at least it's happening right now.

Tom mentioned a lot about the theft and fraud and the criminals they really go where the money is. And they send it back. The weakest link right now we see it's the customer's PC, actually. The customers break in through Trojans and phishing and try to get hold of identities.

Our kind of approach to this is to think of this as a kind of continuous development. We had security measures which are not good enough now so we have to develop and redevelop and reinvest in new methods now and for the future as well. We have to do it.

So we are looking now into launching PKI-based solutions as discussed before. And after that, it might be biometrics, smart cards and so on. But step-by-step, continuously developing our methods so that we try to cope with the threats of the monster that we see around us.

This last the need for collaboration, the need to collaborate in the business, between the businesses, with the government. So we have to collaborate on lots of these issues to be successful enough and not be open to too much risk of exposure.

Thank you.

>>CHIP TSANTES

Hi, I'm Chip Tsantes from Intersections. Many of you probably never heard of Intersections, but I'm sure you've heard of our customers including Discover, Bank of America, Citibank. We're the largest provider of consumer identity management solutions in North America. In addition, we run a background screening business and a few other information businesses. So identity, authentication, proofing is very core to our business and what we do. So every year we authenticate millions of consumers and we do this virtually. We don't have offices, we don't have branches. We do this either on the phone, via the web or other channels like that. We have to be pretty certain that they are who they are because we're permissioning those people to see a lot of valuable information about that individual.

We're constantly looking for better ways to authenticate people and for people to be authenticated and proof coming to us. My problem as the CTO, I've got to figure out from zero to infinity how much money to spend and how much time to spend on security and authentication. I have to be right, in other words stay ahead of the people who are trying to compromise these identities and authentications and stay ahead of the competition that I have as well as the fraudsters who are certainly more motivated.

So authentication, we want to make sure that the person coming in each time is who they say they are. And what's interesting is, when I think I've have a bad day, I'll go down to the call center to listen in to calls, to listen to people who had really bad days because their identities

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 them. They want it convenient and they want it to work for them each time they come in.

As I looked at the marketplace, there are many vendors. And some of those were in the previous panel. I talked to I think all of them as well as probably 40 or 50 others. The problem with all those is if you look at the upper right hand quadrant here to steal something from Gartner, what I want is an authenticated person. A real proof person. I can't buy that. All I can buy is information or tokens or things that I have to put together to make it work, make sure I'm betting on the right ones, is fingerprint better than voice? Is this token better than that token? Quite frankly, my job is on the line to make the right choices here and not go down a dead end, right? So here's a different representation. And the vendors in the room might get uncomfortable, I'm not trying to pin someone in a corner, but, again, there's no way to get what I want from one vendor that's all integrated and works properly.

So I came up with sort of an authentication framework at Intersections where we're looking at the whole thing across-the-board from the initial identity verification through confirmation when you come into the system, make it all integrated and make it work across all of the channels that we do. So I deal with some banks in my own personal life where the voice channel they do differently than the online channel than other things. And it doesn't make sense to me. We do this digging across all our channels making sure that we have the various identity credentials issued and coordinated and then also we have a big effort on remediating through technology and through humans cases that need further investigation. So it's not simply technology. We do a lot with our human investigators to follow-up, to try things, to not send out your whole credit report until we make sure it's going to the right place and you're the right person who ordered it. We do a lot of monitoring behind the scenes to make sure we're not giving things to people that we shouldn't or if someone has ordered 10 of these, that's not a good idea. Actually we don't even let you get that far.

But it's multiple components and it's a framework that allows me to plug and play various pieces of technology around a central data architecture and framework so that we can plug different technologies in. And actually what we're doing now is we're trying multiple technologies, multiple of the components that were talked about earlier and seeing which ones our customers like and then we'll let them vote. And the ones quite frankly that we're having the most success with today are voice, because that's something that most people carry with them and most people have a device and then the mobile phone which again everybody carries with them and people are fairly adept at using and incorporating into their lives beyond just talking.

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 not to spend infinity.

So we continue to live this. And we believe there is a role for government in helping us to share both good and more importantly bad actors or bad identities out there so we can firewall those off and make sure we don't do that.

Our framework I think can work with all sizes. We're a small cap company. We've made it work. And so I think it works well for us and it can scale. And I'm happy to talk to you about that at some other time.

I think the U.S. government can help. And the one big area it can help and it's probably too late for all of us in the room but certainly for my children I'd like the access to PII stopped. There's plenty of places I can go and buy or rent that data and I don't have to be a business to do it. There's plenty of places I can go where there's unintended whether it's classmates.com or ancestry.com where I can go and get a whole host of information about all of you and be able to answer the knowledge-based authentication questions very successfully. I'd like to see a stop to that, as well. Okay, thank you.

>>JEFF KOPCHIK

Thank you very much. As Gail said, I'm the only government person on the panel so I don't have a PowerPoint presentation. So I'm just going to sit right here and give you a slightly different perspective. What I would like to talk about for sort of the five-minute introductory remarks is not so much the guidance that Gail referred to, although I'm going to give you a two-sentence summary of it. But I assume most people in the audience are familiar with it if you're familiar with the topic. But really to talk about what the banking agencies have seen and what the banking industry has done from our perspective as regulators since this guidance went into effect.

So the guidance basically is in the fall of 2005, all the five federal banking agencies in the United States put out a piece of guidance that said to banks that we expected them to use stronger authentication methods for electronic banking systems. And what we meant by stronger authentication was something more than the traditional log-on ID and password that I think most of you were familiar with. And the vast majority of banks were using for, for example, their Internet banking product. And that guidance went into effect January 1st of this year. So we basically now at this point sort of have four months' worth of data or information about how banks, insured depository institutions in the United States, have responded to that guidance.

Now one thing I would like to point out to you is first of all the guidance doesn't mandate a specific technology, in fact it doesn't mandate any technology at all. It simply says you have to use something more robust than a log-on ID and a password and the technology or the technique you use has to be commensurate with the amount of risk that you have in your system so that banks technically when examiners go in, one bank may be required to have a system that's more robust than its bank across the street because its system, for whatever reason, has more risk inherent in it.

I sort of find this interesting. The guidance is referred to by many people as the multi-factor authentication guidance. It doesn't actually require multi-factor authentication. It talks about it. And that is one potential solution. But there are others. So we sort of, in my line of work, consider that to be a bit of a misnomer.

Anyway, that's sort of the background to it. And I would say the first thing that we noticed is that in implementing this guidance, I think it's fair to say that banks in the United States were concerned about two things: They were certainly concerned about cost and, secondly, they were concerned about customer acceptance and ease of use, which makes perfect sense to me. You got to layout a certain amount of money to do this. And you're concerned if you're a banker that you may lose customers because you may make the system of logging on to the Internet and paying your bills so difficult that that customer decides to migrate their business somewhere else. So those are really the two factors that we saw that I think are of greatest concerns.

What are the trends that we've seen? I really put them in two spheres because I think they're different lines of business. In other words, what have we seen in the consumer space? And what have we seen in sort of the commercial wholesale space?

In the consumer space, it's fairly clear to us that the technology that the vast majority of banks have adopted as their primary method of up front authentication is what we refer to as device authentication. In other words, that's using the device, the PC or the laptop that the consumer's logging in from as, in effect, the second factor of authentication. So you put in your log-in ID and then you put in your password. But then through a variety of parameters, and it can be an encrypted cookie that is on the machine. It can be on the IP address. It can be geolocation. It can be a combination of all these. The bank, in effect, identifies and says yes, this is the PC that my customer logs in from to pay their bills. This is the PC that has been enrolled in the system. And the vast majority of banks in the consumer space have chosen to go this way.

I think basically that the reason for that is because it is relatively speaking an inexpensive solution if you compare it to some of the other authentication technologies out there, number one. And, secondly, it is transparent and relatively easy for the consumer to use. The consumer doesn't have to install any new hardware on their machine and they don't have to install any software. In fact, depending upon the enrollment procedures, there's really not a heck of a lot for the consumer to do. And for most people who really think of their PC as an appliance and they

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.

Again, all these things basically work together to help mitigate the risk.

I would point out that from the banking agencies' point of view, one thing that I think some bankers don't realize is that the anomaly detection software, in and of itself, generally does not satisfy the guidance because it does not mitigate against the risk of identity theft. In other words, the hacker coming in to the website getting access to my account and getting sensitive information, all it protects against, and this is obviously a big thing, is potentially money going out the door. So you have to be very careful that that is not a solution that satisfies the guidance sort of in and of itself.

Two more things I'd just like to mention. First of all, generally speaking, we have seen that retail customers in the U.S. are not being charged for this. The banks are paying for it, but every bank that I'm aware of from a competitive point of view has not either added to a cost of online banking or instituted a cost to the customer to use this. In the vast majority of cases in these days, internet banking and bill paying in the United States is generally free.

And the last point I did want to make is that the guidance does not require mutual authentication. In other words, what the guidance requires is that the customer authenticate himself or herself to the bank. It does not require that the bank authenticate itself to the customer.

What we have actually been fairly pleased to see is that there are a number of banks who have decided on their own to basically weave that mutual authentication piece into the system that they've put into place. So they have a variety of mechanisms to try to indicate to the customer that you've actually gotten to the correct website, the website that you intended to go to. And this is not basically a spoof website.

And basically the last thing I would say is that compliance so far I would say is good. It is certainly not universal. I would not tell you that 100 percent of the banks operating in the country today are in compliance. But many, many of them are and many more of them come online each day. So with that I'll turn it back to Gail.

>>GAIL HILLEBRAND

Cynthia?

>>CYNTHIA BOHMAN

Actually I am not a government agency but I also did not bring slides. I was really here to talk about the implementation of some of the technologies that you had heard about on the earlier panel along with the guidance in compliance with that. So I'm sure you can get the mental picture of what that might look like. But with our implementation, I wanted to talk through exactly what we did implement and the approach that we really took as well as some of the components that we thought would be really critical for helping anybody else going through this to make that process go more smoothly.

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 technology aspect of the solution.

The thought around how to do it in a way that would be least impactful to the customer was really from feedback that we actually got from our customers.

So in addition to coming up with what we actually wanted to do from a technology perspective, we also did a little survey of our customers just to find out what they felt was existing security, how their perception was of the existing security, and also what they felt would be acceptable to them if we were going to enhance that in some way.

It turned out a lot of the consumers really weren't very aware of the FFIEC guidance. So from their perspective, this was something just coming at them from all their banks a little bit out of the blue. What we found was when we talked with other banks and some vendors how we explained that to customers was a bit of a differentiating factor for helping people through, making sure they were continuing to use the website.

So some approaches when we got through the survey, some of the key findings that we found were a lot of our customers actually thought the existing security with user name and password was fine. That's probably not a big surprise.

So the other thing we saw was, there was a small segment that felt that it didn't matter what we added, that their identity was probably going to be at risk anyway. So that was another group.

And the third group, though, fortunately the majority of them did feel like they would be amenable to adding some additional authentication as long as the convenience of the channel didn't go away. So that was really top of mind for them and top of mind for us, as well. That was very important to us, too, because in our mind the acceptance on the consumer end -- and they really are a piece in the puzzle. We've heard all the vendors talk through the technology and we've seen all the diagrams of how the technology works and all the closed loops but the consumer is a very important part of that loop. And how they interact with the technology and what they do with it is very important to making it something that gets the game we're all looking for. So that was something that was very critical for us that they accepted it and found it very beneficial.

So with all of those things in mind, we talked with a lot of other vendors, we talked with a lot of the banks to kind of get some of their impression of having implemented this multiple times before we did what they felt were critical for making that go smoothly and we came up

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 straightforward. And any time that anyone interacts with technology, you always have -- there are pieces to it that you'll never predict. Some of the things we've run into after having put it in are things like when we grouped our questions, people use the down arrow key to go from one to the next. That inadvertently selected the wrong question for them in a group they just left. So those are the kinds of things where I don't know how we would have tested that or how we could have come up with something to avoid that. My understanding is technology-wise you just never quite know how people will interact with your web screen. Those are some of the things that have come up. And that's where the part about not having everyone do it on day one was really helpful for us. When we staggered the enrollment, we were able to tweak our instructions a little bit, change some of the scripts in terms of questions that came into our call centers and really try to allow for those things to change over time so that by the time the majority of our customers were there we had at least gotten a little better about answering those questions and really trying to deal with that.

I think the important part of consideration is also thinking you're training people to do something that's new. So the other part we thought through was how to chunk the information out where it wasn't trying to send someone a note that they had to read all at once because we also know consumers just don't read what you send them. They don't read it fully and digest it all fully. So we really tried to send a little bit of it at a time. We sent two weeks before you had to, before enrollment, we didn't allow the customers to access the website before going through the enrollment process. We would send them an email and really highlight the benefits. When they got to the enrollment phase, that's the point where we really tried to make the instructions clear. And then we've actually created a security center on our website for anyone who wanted a little extra information.

So in conclusion, we're about halfway through enrollment now. It's actually gone

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.

I also want to point out that there are lots of relevant standards -- the NCUA, FFIEC guidance and payment card industry standards as well. Most of us are using all of those as self-assessment guidelines and subjecting ourselves to continuous independent assessment to make sure we're constantly meeting those requirements.

I recommend that as a management strategy most highly.

I'm going to skip right by this. I just throw it up here because technology is part of the solution. Lots and lots of technology. And it's very easy to get lost in the technology. But people are the real answer here.

I'll just talk briefly about this one because it emphasizes something that Cynthia just brought up, which is you can put out information to your members all the time. You can train your staff all the time. You can send out emails. You can send out newsletters. You can hold Webinars. You can do everything. But they will not pay attention until just before it's time to make a change. We're all human beings. I think we understand the reality of that. We don't change unless we have no choice. So we don't tend to pay attention to this information until we have no choice.

One thing I do want to mention, it was mentioned earlier, which is that part of the problem is having clear processes and people trained in those processes to administer them. That's where your staff orientation and annual refresher training comes in.

So now let's talk about our experience with multifactor authentication. I think another way to look at the bottom line on this chart is our objective was to inspire confidence and trust in the security and safety of our online banking systems. This was not about meeting regulatory guidelines. It was about honoring our commitment to our members.

But rolling out anything such as MFA requires comprehensive and extensive preparation. However much you think you know about it, you can't do enough.

We started out, Cynthia you said you started out like a month or two or something like that? We started out six months in advance sending out newsletters. Putting inserts in. Holding web sessions. Holding local training sessions at our branches. "Here's what's coming and you need to get ready."

We set out all of the media that everybody would always think about, knowing full well that we'd only reach a small percentage of people because most of them would wait until the last minute.

We invited people to be beta testers. Don't use technologically sophisticated people to do this. They're not going to find the problems that the average consumer or member is going to

trip over.

We generated FAQs, frequently asked questions. Not only for the call center but for everybody in the credit union so no matter where a member showed up or where they called, we would have those answers to those questions. And we trained our staff relentlessly on the likely issues we expected to encounter and how to assist the members. And then we advised everybody that as soon as we started rolling everything out, it was all going to change, because within the first two to three weeks of rollout, we had encountered a whole bunch of issues with our members implementing MFA that we hadn't anticipated. It was very important to have preplanned, I'll call it a rapid response team, that took each of those issues, resolved them, figured out what we needed to say to our members to help them get through that and rapidly transmit that to everybody in the credit union so no matter where a member went for help, they would get a current and correct answer.

We did, like Cynthia, give them time to transition. But we did set a deadline. So everybody knew that after a certain date, and it was three months, the system would be live and you couldn't log-in with a user name and password. So we gave them a transition time. We even gave them a demonstration system on our website. MFA is coming. Log-on here and see how it's going to work. They could just play with it with no consequences. Some people did, some people didn't.

The other thing that we learned was: you've got to commit a large number of your staff to answering phone calls and inquiries from members right after implementation. If you can get to them quickly and address their concerns, you maintain their trust and inspire their confidence. And then they will use the system religiously.

This is just my personal opinion. This issue is not going to go away. I do think because we tend to absorb the cost to protect our members that those costs will rise as the threats get worse and the technology we have to deploy gets more sophisticated. And like everybody else who's been up here today, I see a mixed market of solutions. And I think a growing opportunity for some biometric approaches. Key stroke logging, key stroke dynamics and things like that, there are all kinds of techniques that are evolving that have a lot of promise. Thank you very much.

>>GAIL HILLEBRAND

You're very good to keep it very short so we could have Q & A. I'm going to address most of the questions to two or perhaps three of them although they're all questions that any of them could answer. The first one is for Bjørn and for Cynthia. Tell us about the business case. How did you get your companies to spend some money, some serious money on better authentication? And Cynthia put aside for a moment the regulatory requirements and talk about the other things. Bjørn, do you want to take that one first?

>>BJØRN SKJELBRED

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. But it's the feeling that the money will be lost. So the difficult thing here is to try to quantify the trust image, how much it is worth.

>>CYNTHIA BOHMAN

I think I will agree with that. One thing I would want to point out too is when we explain the benefits to our card members about why we were doing this. It really wasn't about that we were making sure we were regulatorily compliant. That's not really the part that made the most sense for us, it's not really why we did it even. We, also, again, it's the reputation we have, because people are providing very sensitive information to us. Frankly, they're giving their money to us. That's always something that we need to make sure that we're building confidence in them that we're taking all the right steps and we're doing the right things. In our business case model, those are factors that get weighed in. Any new bright idea that anyone has in our company, it does go through a process where it's not just a black and white cost benefit model. There's weighting to how can it help enhance our reputation? How can it also help potentially a customer irritation or something that customers – that could be done to be more convenient for them or secure the data and also help to reduce some of the fraud as well? So anything that pulls all of that together, it wasn't extremely hard to get that through.

>>GAIL HILLEBRAND

The next question is for Tom and for Jeff. Do you see authentication and privacy as complimentary or contradictory? And how can we make them more complimentary?

>>TOM KELLERMAN

Go ahead, Jeff.

>>JEFF KOPCHIK

Thank you. (Laughter.)

Well actually before I answer the question, I would just like to say that I was shocked at Cynthia's statement that consumers don't read FFIEC guidance. (Laughter.)

I can't conceive of that. If they did, there would be no insomnia. But anyway, in terms of the question, I tend to think of them as complimentary in the sense that I mean I truly believe that to the extent that stronger authentication helps to protect this information and make sure that the wrong people don't get access to it, that that ultimately does, in most cases, promote privacy and is something that is good for consumers and anyone who does anything online. I understand the tension between the two. But I think really ultimately that's what everyone who has spoken today is really trying to do. So I mean I think of it as, yes, it does promote it and they

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 for identity theft prevention? Or was that a standard developed for antiterrorism, money laundering, we ought to look at something different? Cynthia do you want to start with that? And then I'll take Jeff and Dick?

>>CYNTHIA BOHMAN

In terms of the standard of not all things match and so forth, I think the challenges in what we heard this morning is that the documents are such that even when you are a legitimate person, there are always reasons why things don't necessarily -- I think there was a lady in the last session who talked about being asked about her investment properties in terms of trying to give some information. So I think we always have to, on some level, allow for that. But then to Dick's point, we do have to monitor it. We have a lot of manual processes as well. And I think you -- it's manual and that's probably the more expensive way to do it but at the moment there isn't a perfect technology for it. So the manual process allows you some flexibility when trends change and that kind of thing, also. I'm not sure there's a way to be very precise with that kind of thing, as well. Because you're dealing with more or less people and that's always where the imprecision is there.

>>GAIL HILLEBRAND

Jeff, on this question?

>>JEFF KOPCHIK

The only thing I'd like to add is I'm a little hesitant to sort of analogize between anti-money laundering and bank secrecy act and, sort of, authentication in the way that I think about it and work with it. But I would echo what Cynthia said, which is in any of these systems, there is rarely sort of the 100 percent perfect match. And I think the key is to structure the system in such a way -- and of course the bank to a certain extent or the bank's vendor can, for lack of a better word, turn the dial in terms of how far do you want to ratchet it up? And that's a risk decision that the institution in my world has to make. Do I want it to be 90 percent sure that the customer is who they say they are? 85 percent? 95 percent? Of course I have to balance that

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 exercise in futility. So what we talk about is a system of compensating controls. And people making judgments based on the information available and having those judgments scrutinized by experts based on other information having to do with behavior or other secondary sources of information that may become available so that no decision like opening an account based upon apparently valid but fraudulent credentials will stand for long. It may stand for a while, but it won't stand for long.

And again that's the concept of a risk-based approach. If you tried to get it right 100 percent of the time, then it's going to cost too much and inconvenience too many of your legitimate customers and members, and that's not productive, either.

>> GAIL HILLEBRAND

The FTC told me before we started that we could have until 5:30. I'll ask two more questions and we'll see what kind of questions you have and if you haven't got any, we have a few more. This next one is for Chip and Tom. Now I'm trying to figure out where it is. Oh. Tell us about work-arounds. What do you do when the technology is so perfect that people take shortcuts that undermine it? And I'm thinking of the lawyer I know who told me "yeah, I have a friend who has a different password for every financial account and he's got it all on a file in his home PC."

That's the one we could predict. How do you design against and predict the customer work-arounds so that they don't undermine the technology? Chip, do you want to start with that one?

>>CHIP TSANTES

Yeah, again I think that we do a lot of testing, as well, and get our customers involved. But, again, I am amazed at how clever customers are in working around these things. You don't want to design it so difficult that the password is so complex, you've made the password so complex that they all forget it. And then you're back where you started from and asking their mother's maiden name or something to reauthenticate. We don't do that. But you have to strike

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 are human errors, human mistakes -- the human is not following procedures. So we put a great emphasis on training, retraining and constantly oriented -- we have sort of a stated philosophy at our company that everybody works in the security department. It's everybody's responsibility. And we just hammer them and emphasize and reemphasize that. Not just the first day you come in, the first

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 briefly in the morning. I got part of the Real ID conversation. But I believe that a lot of that would help us, I think, with the generation of accounts. More so than validating our existing customers which is what I think the topic we are focused on discussing now.

However, that is a whole other area that does need to get looked at. And to the question earlier about is it right to have something only be specific or maybe just a percentage accurate not 100 percent, it might notch that up a little bit. So from that perspective, opening the account, and that's where a lot of it starts. Anything you can take off that will trickle down.

>>GAIL HILLEBRAND

Dick?

>>DICK POWELL

I think Cynthia's right. I think from a process and procedure point of view, it would streamline things considerably. Exactly how much? It's kind of hard to say right now because we still have lots of rules and regulations that govern our behavior and lots of examiners and auditors who come in and make sure we follow those rules.

So I guess that gets to process, right? If something changes fundamentally in the space called validated identification and what implications does it have for the way we all do business based on another model of lack of trust in the documents that we're presented.

>>GAIL HILLEBRAND

I saw another question over here in the middle somewhere, yes.

>>AUDIENCE MEMBER

Jeff, now that we've seen compliance to the first round of FFIEC guidance, I was wondering if you could comment on how you think the guidance will evolve over the next couple years?

>>JEFF KOPCHIK

Well as I mentioned when the FFIEC agencies wrote the guidance, we deliberately did not mandate a particular type of technology because we made the assumption that if we did, I mean there are many reasons not to do so, but the one I was going to really focus on was the idea that that technology, whatever it is, is going to change within the next year or two because as everyone has said, this is a cat and mouse game. This is a continuum. What is very, very good technology today that will meet the guidance will probably not be acceptable. Pick a number. Two years from now? So what I see is the idea that examiners and bankers are going to have to basically try to keep up on what is it that reaches that acceptable level? And most of the

technologists that I've talked to -- now keep in mind, in the banking world, most banks don't do this on their own. Most banks go to one of eight or 10 major technology service providers from which they get their Internet banking product. And every one of the eight major banking providers that I have talked to who is designing these authentication systems is doing it on – and someone mentioned this earlier before lunch – on a plug and play basis. Which is the idea that you have your authentication piece and right now you're using device ID. Well say that gets compromised two years from now and it's no good. You basically pull that out and you plug in the next, more robust technology without disturbing basically the rest of the system you have put together.

So what I basically see is these technologies just constantly being upgraded and changing. And banks every couple years basically augmenting it, rolling out something that is quite frankly newer and more robust that is going to cost a certain amount of money. But they're going to have to do that to keep ahead of the fraudsters and basically to keep themselves in compliance with the guidance.

I mean I wouldn't even predict where it's necessarily going to go other than to say I mean personally I think that you're going to see, because the costs are coming down, more of the use of the one time password tokens in the retail space than you do now. It used to be cost prohibitive. Those tokens used to be $100 a pop. They're now down to like $5 a customer or less. As it gets down to that level, then it starts to become much more affordable in the consumer space.

>>AUDIENCE MEMBER

It sounds like guidance today states that you have to do something better than a log-in ID and password. Which doesn't necessarily mean that somebody has to keep up with technology. But it sounds like from what you said you think the guidance is written such that it's written to be able to evolve?

>>JEFF KOPCHIK

Absolutely. I mean I picked out that one line from the guidance, but if you read it carefully, there are other sentences in the guidance which I think make it very clear that it has to be commensurate with the risk and it's a living document. Like I said, we didn't -- any of you who have been involved in the interagency rule making process or guidance process know that it's extremely painful, very time consuming, and if you're me, you don't want to go back into that room again two years later. So you are going to write the document in such a way that you don't have to do that.

>>GAIL HILLEBRAND

I have one here, one in the very back and a couple over here. Go ahead.

>>AUDIENCE MEMBER

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

Well the answer to that question is there are a number of reasons. It mainly depends on why -- well, a couple things. It depends on why you're not in compliance.

For example, are you not in compliance because you read the guidance and threw it in the circular file and just decided to ignore it and you made a conscious decision that you weren't going to adhere to it? That's one scenario that I would suggest to you that most of my federal bank regulators would not be really happy about.

Or are you not in compliance because you are one of 200 customers of a particular major service provider, that service provider and your institution worked very diligently to get to the point where they had everything in place by the beginning of the year, but then what they decided to do was to do a rolling implementation because you don't want to turn the switch and bring -- pick a number -- 10,000 customers online on the same day. You want to do it staggered.

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. Or that they looked at the guidance, knew that they were subject to it and perhaps -- and this is the minority of cases -- for whatever reason, just didn't really do much about it. I mean those are the ones that we're concentrating looking at.

And I sort of missed the last part of your question. If it's does the guidance apply to telephone banking? It does. And the regulators have purposely sort of decided that we're going to look at the Internet channel sort of first and foremost because that's the one that most consumers use and give banks a little more leeway on the telephone channel because less customers use it and it's generally considered to be less risky. If that doesn't answer your question, I'll try.

>>AUDIENCE MEMBER

It partially does. A – has it been a more rigorous time frame set around telephone banking? And do you think that the enforcement or the correctional actions that are being taken against those that have not done anything, not those that are just part of a phased rollout, are they enough of a deterrent for the other FIs to continue and say to adhere to the guidance?

>>JEFF KOPCHIK

I think the first part of the question is I think the regulators in general have given banks a little more leeway in the telephone space than they have in the Internet space.

And I think in terms of the second part of the question, I think that, yes, every banker and credit union, for that matter, knows that when the examiner comes in, whenever your next exam is, this is going to be one of the first questions they're going to ask. It's on every examiner's checklist. The examiner is going to want to know: show me what you've done and where you are on the process. And bankers know, because they talk to one another, what sort of has happened to their colleagues who perhaps have not pursued this as vigorously as we think they should have.

>>GAIL HILLEBRAND

Great. Was your question answered, the man in the white shirt, you had your hand up for a while, was it answered?

>>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 gentleman on the left, sorry I'm bad with names. There's the universal "man-in-the-middle" kit, which is already compromising OTPs, that is foiling the picture and the password and the cookie and the device. Most of what has been proffered today is already busted. When should we be looking for FFIEC 2?

>>JEFF KOPCHIK

Quite frankly that's really not a question I can answer. I would say this: We constantly look at the guidance that we put out. And we try to figure out, you know, is it something -- actually this authentication guidance repealed authentication guidance that was put in 2001 because the FFIEC agencies came to the conclusion that that guidance was simply outmoded. So we are constantly in a mode of sort of looking and saying do we need to do something new. That being said, we don't like to do that on a yearly basis because it has sort of a destabilizing -- it may be too strong of a word -- but a destabilizing influence on the industry. You don't want to keep coming out with new stuff because bankers justifiably say we can't keep up with this. That's why we try to write it in a flexible manner such that it would survive, I hope, for at least a few years without major modifications. Other than that, I really can't comment on what's coming down the pike.

>>GAIL HILLEBRAND

I'm going to ask Jeff to stick around after and take additional questions about the guidance because I think there are some more. Let me just say, as a consumer advocate, if you're out there and your own technology department is putting up web presentations saying these systems are broken, current authentication isn't good enough, we're going to be looking for you to do more whether the regulators tell you to or not. So there's another question there.

There's one question that the FTC asked me to make sure the panelists covered. I'm going to ask that one then we'll take a few more of your questions. The question is: when there are multiple channels for authenticating, and let's make it even harder, there are multiple product lines and multiple decision-making processes within your financial services group or institution, I won't ask you how you're doing it, but how do you think it should be done? Should it be done with the IT Czar who tells everyone what to do? In which case how do you get buy-in? Or should it be done with product line by-product line, channel by channel? In which case how do you learn from each other? Cynthia do you want to start with that one?

>>CYNTHIA BOHMAN

I can say in our case actually because we do have multiple product lines, though the card is one of those, we have loans, we have a bank, we have multiple ones in there.

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 don't want that."? Personally I can attest to that because I have several financial institutions that say you call this 800 number and we won't send your data. I got other notices saying we're going to send it to whomever we want under Gramm-Leach-Bliley. Since that was 99 and we're now into the year 2007, both from institutions making a change to saying giving a little bit more to the consumer to decide to opt out or from the regulator side. Any thoughts on that? Given the extent of the fraud, identity fraud, what's happening out here in the outside?

>>GAIL HILLEBRAND

Who wants to comment on affiliate sharing and Gramm-Leach-Bliley.

>>TOM KELLERMAN

I'd like to speak to that. There's numerous regulations around the world for the financial sector that are actually more robust where it's opt in. Opt out stinks because you can't really opt out. Half the time you are calling a call center trying to figure out when I can opt out. It should be opt in. And HIPPA is opt in. So I don't understand why GLBA is opt out. HIPPA is the healthcare law for information privacy and protection.

>>AUDIENCE MEMBER

To make it more relevant we should mention class-based documents. Information goes to the third-party marketers. The marketers what controls are there now? And where are the data brokers? A lot of it is crossed, have I got the correct name and address? The data broker gets from lots of sources.

>>CHIP TSANTES

Again, at our company, we only get data that we're permissioned to get for our customer, whether it's a one time or an ongoing relationship and that's it. We don't reuse that at all. I would like to see data strip mining go away. It's just that simple. There are people out there strip mining that data and making it available in all kinds of ways that have intended and unintended consequences. And it needs to stop.

>>GAIL HILLEBRAND

Chip, give us something to dream about overnight before we all come back tomorrow?

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.