Jim McMahon: My name is Jim McMahon. I work in the technology office of the U.S. Department of Education, Federal Student Aid. With me today is Steve Burke who also works in the technology office. We're here to talk about two-factor authentication.

So I'm gonna ask a couple questions first. So who's heard of two-factor authentication before? Did you hear – I was about to say did you hear about it before you came to the conference? No. Okay. Well good. We'll all learn something together then.

So how many folks are actually from the IT shop at their institution? And the rest I'm assuming is business generally? Okay. All right. Fantastic.

So we're basically gonna cover three major topics, which is what is the problem that we're trying to address here, what is the solution for that problem and then really some of the high level what and when of that's gonna happen, which is probably the part you're most interested in. So you can talk to Steve about that.

So you can see on the slide there's a bunch of words about O&B telling us things. Basically, what things boil down to is the mission of federal student aid and your mission is getting the right aid to the right students at the right time. That's what it basically boils down to.

In that role, we have to receive, use, process, store personally identifying information, which is something that over time has become more and more valuable. Why? Because basically there are people out there that want to be able to take that information and sell it for their own use. It's really that simple.

So we, we being you and the Department of Education, have an asset that belongs to our students and our citizens that we're responsible for protecting. So really, what OMB is trying to tell us is there are certain things you need to do as a steward of not just the taxpayer dollar, but the taxpayer information to make sure that it is being protected appropriately. So that's really what two-factor authentication is all about and I'll get into a little more detail.

So before the conference we had our software developers' conference. We actually spent the whole day discussing security, security posture, risks, all that type of things. So the information up on the screen gives you an idea on what we're talking about in terms of the amount of data that we're responsible for at Federal Student Aid.

You can see we have 6,400 unique institutions, 3,000 financial partners, over 90,000 privileged accounts and I'll define that in a second; 70 million, probably actually closer to 80 million unique IDs, et cetera, et cetera, et cetera. We're basically the world's sixth largest bank, which is a lot of information.

So if there was someone who wanted to find information about people, maybe even younger people, we're a pretty ripe target when it comes down to it. There aren't that many bigger in the federal government than Federal Student Aid. Obviously there are SSA, IRS, some of the others, but we're kinda' up near the top.

Alrighty. So, this is the cost of a breach. The numbers you see there are what the general retail value for those pieces of information are if I was to somehow get some of that and be able to sell it online somewhere. Those are just ballpark figures. Obviously, they change a lot. The last one is the only one that is not. That is the average impact to an individual who actually has had their identity stolen.

There are also costs associated with the folks that actually were responsible for keeping care of that data. What we heard on Monday was that the average cost of a breach, the hard cost, is about $7.2 million and that's because there's steps that need to be taken to remediate security posture, there are steps that need to be taken to make those people that have had their identity possibly stolen or possibly compromised whole again in terms of credit monitoring, reporting, et cetera, et cetera.

That's just the hard costs. That's not the costs associated with the impact to reputation, the loss of possible student attendance or revenue, depending on if it's a business or a school, et cetera. So there are significant costs. It really is an area that gets a lot of attention.

One of the concepts behind two-factor authentication as opposed to a lot of the other security steps that we take is – the mindset should be such. This isn't necessarily about keeping networks safe and those types of things and we spent a lot of time talking about that. This is really all about a certain assumption.

Well, let me just ask. Has anybody ever heard of key logging? Okay. So key logging is a relatively basic concept. It simply means that somewhere, somehow someone has put a piece of software on either PC, network, mobile device that basically

captures all the activity that happens on that device, including all the keystrokes that are done and is then able to exfiltrate that information out to someone else at a different computer somewhere else.

So really what that means is with that set of information, which with capturing those keystrokes they're able then to determine which of those look like user IDs and passwords, which of those look like SSNs, which of those look like et cetera, et cetera.

We have an ongoing process in the federal government through U.S. Cert that actually does a lot of monitoring _____ and we actually get reports from U.S. Cert on folks they think have had a key logging issue and they send us the names of those folks and we contact them on an ongoing basis.

What two-factor authentication is trying to address is let's just assume, worst possibility, that that kind of infiltration's already happened. There's already key logging on your systems or our PCs or somewhere. So when you're going on and you're logging onto a particular system right now, you're just using user name and password. That's what they call a single factor.

Now, the factors of the authentication, multi-factor authentications basically there are three factors. There's what you know, what you have and what you are. What we've made a determination on based on guidance from FISMA, ANIST – you don't have to worry about those acronyms. Those are the people that tell us what we need to do in terms of security. Is use two factors.

So the what you know is you use name and password. This is not, as Steve will tell you, this is not actually a foreign concept to what happens in your daily life in terms of when you go to the bank and you use your ATM card. Your card is a second factor 'cause it's something you have and it's something only you have and it's something that you have that only works in conjunction with the user name and password that you know. So that's a second factor.

We're not gonna move into biometrics, retinal scans, those types of things. Hooray for us. So that's the other factor. Then certainly our federal agencies, not us, that are required to use those all three factors because the type of information they're securing could have significant impact if it was leaked.

So, what we're simply trying to do is make sure that we're doing the best we can. Putting the insurance in place that we can.

Putting the protections in place that we can to make sure that the data that we all access is secure.

On a day-to-day basis, given the amount of folks we deal with and given the amount of information that exchanges hands, I think often what happens is we become a little desensitized to exactly what the possible impacts are if that slips out. I know I certainly do.

I know if I look back over my career at Federal Student Aid, having CDs that have the Pell recipient file for entire years sitting in my desk somewhere. Not something I'm comfortable with, but we are taking steps to make sure that type of thing doesn't happen and if it does, there are extra steps then that make it harder because if someone has that key logging on and we have two factor in place, two factor, and Steve will show you, is basically with us our second factor is a key fob.

It's a key fob that generates a six-digit number so that if somebody was going through and capturing that user name and password and then they were capturing that six-digit number, that six-digit number changes every minute. So they're not gonna be able to gain any additional access into your accounts because they only have one of the factors. They don't have that third piece of information.

So they could go ahead and try that six digit number they've captured, but it's not gonna work for them. So that's what the protection piece is of two factor.

So, I'll try to get back on the slides a little bit. So provide safe and secure access to all FSA networks and services. These are the communities that we deal with.

And I'm sorry. Let me jump back once second and define the privileged users. We basically break our world into two sets of users. There are non-privileged and those are simply the folks that can see their own personally identifying information. So, students, parents.

Then there are folks like you and I who actually can access systems that have lots of other people's personally identifying information. That makes me a privileged user. There's a risk there, right. I can see other people's identifying information and if I was an ill-intended person, do something with that. So that's

why we have different rules for privileged versus non-privileged users.

A lot of our privileged users fall into that second bullet, which is schools, subcontractors, GAs, servicers, PCAs, NFPs, et cetera. So the scope of the two-factor project that we're working on is simply for the privileged users. This is not about students or parents. This is simply about us folks that can do more harm than other folks.

So what you see on the screen there is a picture of what the two factor token is gonna look like. It's simply a little fob that goes on your keychain. Like it says, something you know, something you have.

It generates what we call a OTP, a one-time password, which is that six-digit number. Let me see if I can do a half-decent job of explaining 'cause we had a lot of questions. How does it work. You wanna take that?

Steve Burke: _____.

Jim McMahon: Alright. Then I'm gonna sit down.

Steve Burke: You don't have to sit down. _____ _____ that's all.

[Mic not on]

Steve Burke: Technology is great when it works, isn't it? Fantastic. We'll put that one off there.

I realize that this is Friday morning. I realize I'm between you and the airport, okay. Got that. Jim and I also realize we drew the wrong straw for Friday morning so we have to figure out how to do that, how to get earlier on the schedule next time.

My name is Steve Burke, as Jim has mentioned beforehand and I'm running the two-factor authentication project. Look, I'm gonna start by saying I need your help to do this. This is not something that Steve is doing or Jim or Bridget Ann or Andrew or Bernard or Jennifer or any one individual.

Security is a shared responsibility for all of us. As Jim very eloquently said, we have a lot of records, we have a lot of people, we have a lot of data.

I asked somebody earlier on in the year to help me with this project and because of that person, I wanna recognize her right now. Hopefully she's in the room. Barbara, are you? Barbara Bickett from DeVry University?

Barbara Bickett made it happen for us. We have to go through this attestation process with attestation understanding who you are for the token. Who needs tokens in your school.

I called Barbara up and I said, "Here's that two factor authentication project. We need to lockdown our systems. I need your help. This is how I see it should work." She said, "Well wait a minute, Steve. I have another way. Send me the list of people that you have." I sent her the list of people we have for all of DeVry University. We together went through that and made sure that those people are actually still at that school.

She said, "Got it. Great. Send me the box of tokens." I said, "Okay, wait a minute. You're gonna distribute the tokens throughout your organization." Made it a lot easier for me. So guess what we did from that standpoint? Together we worked together to develop the training, which you're gonna see today in a few minutes.

We put the training materials together for it and as of today, her DPAs and FAAs across the country all registered their tokens. It's very easy. Very few minutes. So kudos to Barbara and the DeVry team. Thank you very much for making it happen. *[Applause]*

As Jim had said, two factor authentication. Multi-factors. There's a lot of different things that are out there. There's facial recognition or fingerprints and be glad that we're not doing the fingerprints because if this gets compromised for some reason, this token, we can disassociate and get a new one for you, but if your thumbprint is compromised, I have a little issue with that.

Now this is my first time being at the FSA conference and I've had a blast of a time learning a lot from a lot of different people across the country. One person came up to me the other day and I was surprised at this one.

He says, "Well we don't wanna do two factor authentication." I said, "But we don't have a choice. Really, we don't have a choice because we need to protect our systems. " He said, "But I'm already doing it." I said, "Really. How are you doing it?" He

said, “Facial recognition on his PC.” I’m like, “You’re kidding me.”

So he said, “No, no.” It was a community college. I won’t’ tell you what state it’s in. Doesn’t really matter, but the fact is they have taken the understanding and understood now the importance of this data that you’re holding. Now they’ve gone to the enth degree, facial recognition. Could you image me or our team trying to sell everybody, 6,500 schools, 60,000 users, you need to have a camera on your computer. Not gonna happen.

Because of that, we still need to have the right type of software, the right type of protections. Our key fob token.

People have walked up to me and asked me a couple questions about the token. “Can you follow me? What are you doing? Are you tracking me?” The answer is no. No. This token is – let me back up a second.

Jim asked the question about two-factor authentication. Have you guys familiar with it before the conference and Jim gave an example of an ATM card. Not everyone has an ATM card, but I guarantee you you’ve been doing two factor authentication in your regular life.

When you checked into this hotel, they gave you one of these, right? Room key, correct? Yes. No. Alright. Okay. Good. I know it’s Friday. Before they gave you the room key what did they do? Attestation. Who are you. They also asked you for a credit card to make sure they get paid, but that’s another thing.

So now, they gave you the key. On this key, there is nothing about you on the key. They took a piece of paper and wrote down the room number. They did not tell you audibly why because someone next door or standing you in the aisle next to you could hear that. It’s important for them to write it down. That’s the know. The have and the know. Something that you have and something that you know.

So when I asked the question or one of you asked the question, two-factor authentication, yeah, we’ve been doing it for years. We’ve been checking into hotels. Moving to higher education, we’re doing the same type of a concept.

What I need you guys to help us with and we’re gonna walk through this is the attestation part of the tokens. With these tokens

there's an algorithm that runs on it. It doesn't talk anywhere else. There's no radio frequency. Basically, it's a room key. You can't do anything unless you have that token with something else.

Another question that came up to me is, "What happens if I lose my token?" Well we're gonna show you the actual registration process and what happens and how you can get that one-time password that's six digits, if you lose your token. We can send it to your Smartphone. We can send it to an e-mail address. Good so far? Alright.

My team when we put this together there was a 43-page document on how to register your token and how to maintain the token; 43 pages in typical fashion. So I said to the team, I said, "Well, we gotta make it simpler. How do we do this? Let's bring it back down."

So my team went back to the table and they narrowed it down to basically one page, which I believe it's one of the handouts that you guys have. That's how you register a token. Now, without fumbling through the papers I'd like you to just watch the screen. We're gonna go through this right now.

So when somebody asks you, "have you been trained on two factor authentication?" The answer is yes. Alright. When you look on the screen right now, you're looking at what we call CPS FAA web access. Top right hand corner it says, "Register maintain token." Click on the button. That's there right now.

The next thing that we're gonna ask you is say, "Okay. First name, last name and your desk number." Now, those are required fields 'cause you see the little asterisk. Also, the e-mail at the bottom. However, we suggest that you give us your cell phone number and I'm gonna come back to the reason why. It's important and we wanna try to do that. Not required, but probably makes sense to you guys.

Next step: on the back of the token what we will have is a serial number. It starts with AVT. Very small number, but you put it in there. Put that number on the computer or on the screen. Then after you've put that number in you answer five challenge questions just like you would with your G-mail account or a bank. Are you following me now? Okay. Five challenge questions.

Then terms of agreement. Basically, it's the same terms of agreement, the rules of behavior that we have throughout all of our

systems. It means you're gonna take good custody of the token. You're not gonna dip it into water or damage anything, even though it's a token. We need you to take good care of it.

The next thing we want you to do is flip that token over. When you flip the token over there's a little button on the left hand side. Push the button one time. A six-digit number will appear. This is the one-time password. Pause a moment, 30 seconds. Push the button a second time. A new number will generate. Put that in the second field.

Then you hit submit. You guys have now completed the training for the two-factor authentication. That's it. But what did we do? What did we do? We took the token. First off, we did the attestation process. We're asked how many people at your school with the DPA. We will send the DPA list of people, let's say these ten people we have on your team. My team will then send you 12 tokens.

You pull one of the tokens out of the drawer for yourself. Jamie takes the token out. First thing we did was put Jamie – your name into the screen, right. First name, last name. Put that contact in there. That's creating the beginning of the profile.

Then you put the serial number of the token that's in your hand. So we have that part.

Next thing we said if you lose your token, how do we get it back? How should we let you know what your one-time password would be? That's the five challenge questions.

Now, remember I said beforehand about why we'd like you to put your cell phone in there? If you put your office phone in there and you're at home, it's not gonna be very helpful. However, if you put your cell phone on there, that phone number, if you lose your token and you need to get your one-time password, it comes to where you are with your phone. Not required. Highly suggested.

You're gonna need to have these tokens to use to access our systems. So people have asked me the question, "Should I leave it at the office? Should I leave it here? Should I leave it there?" I keep it on my ID badge and I keep it with my keys. So when I'm working remotely, there it is because you're gonna need to have this to access our systems.

The tokens are individual. One person to one token. You can't switch the tokens. Now, once again, what we did we have Jamie's name, then we have the serial number. We know where to send Jamie your e-mail, your one-time password if we lose it. We're set and ready to go.

Jamie, your token is specifically to you. Nickie, your token is different. Remember the screen that had the yellow button? The algorithm? Alright. It's an algorithm that runs on here. When you hit that button, it appears to you and I to be a very random number. It's really not random.

On our servers on the back end, we have the same algorithm. When we did that, you pushed the button the first and the second time, along with that serial number, we said okay, I'm starting here. This is Jamie. Here's my first number. We said, "Okay, great. Give me a second one to make sure."

So now, both Jamie's token and our system are synced. So what that does is if Frank picks up Jamie's token and tries to push the button, he can push the button and a number will generate, but can Frank login with that? No. That's because it's assigned to one person.

So when we talk about the tokens we wanna make sure that tokens are not to be shared between individuals. It's one token per person regardless of how many accounts or regardless of how many systems that you're actually entering.

So what have we done? If we look on the screen here, the first two fields, our current day today. In other words, user name and password. That is the first factor. Jim was talking about that. That's the credentials that you have right now.

All we did in this registration process is add that last field. It's that last field that says, "One-time password." The one-time password is when you hit the button. That's the number. So if there is key logger software on your machine and it hits that one-time password, picks up that six-digit number, it won't work because it only works once. Questions. Am I moving too fast? Are we good? No? Okay.

We have two different paths as we're going forward with the two-factor authentication project. There's two different work streams. One stream is when we are enabling the systems. The second stream is when you're actually getting the tokens.

What we're looking at here on the screen here is CPSFA web access was done earlier this year back in April. COD was enabled. However, it's not visible at the moment. We're gonna come up to that momentarily.

On December 18, NSLDS will be moving behind Ames as well. So it will be two factor enabled. Then come February we have the following systems: FMS, SAIG and Ombudsmen.

Where are we right now? As I said, we started earlier in the year on this. We started out with 1,300 FSA associates. My fellow team members, we deployed the tokens on that side.

Then we said, "Alright. That's working well. Let's give them to the 5,000 associates that we have over at the Department of Ed." Alright. Perfect.

Then I called my friend Barbara at DeVry. I said, "I need your help." And that's what that is right there. So she confirmed the users and the tokens went out the door. Once again, thank you Barbara for making it happen for us.

At the same time, I reached out to my team members to handle the foreign schools. Now how many of the foreign schools do we have in the room? Excellent. You guys have gotten the token? Excellent. We're underway. Thank you very much.

As of this morning, the count is 923 foreign schools have registered their tokens. Thank you. It is a Herculean effort to make sure that we got it not only to you, the right place in some other country, but you guys have registered. So we're greatly appreciative.

The next phase of our project is to tackle all of the schools domestically. We broke the schools out into nine groups. The first groups are D.C., Maryland, Virginia, West Virginia and our own backyard. Now, this is the end of the month. Not the beginning of the month. So by 12/31 that's when we wanna have all the tokens out to the domestic schools in these states.

My team has already started the attestation process in reaching out to you. Some of the schools that I've seen here, Maryland and others, we're gonna accelerate the process.

The biggest challenge we've had so far is the attestation phase. When we sent the e-mails out to the teams, to the primary DPAs who were leveraging saying, "Okay, guys, how many people do you have?" That should be a very short and quick answer. These are the number of people that I have on my systems and oh, by the way, I'm giving you the list of what I see. That's okay. Send it right back.

I had one school that took seven weeks to reply back. They said, "Oh, I didn't think this was important." This is important, folks. Definitely important.

On the next screen here this is how our team has broken out the different groups. Like I said it's nine different groups across the entire country, including Puerto Rico and some of the other territories.

Now, the way that this is laid out is based upon, for my own sanity, from where it says D.C. at the very top there to where it says Wyoming at the bottom, that's 60,000 tokens.

Now how do we do this? It's broken out based upon roughly 800 to 1,000 e-mails that we have to communicate with the DPAs each month. So it's not alphabetical. It's not by the size of the state. It's not by the number of schools. It's based upon the number of DPAs that we're gonna have to reach out to.

A few different steps; internally and externally. Our presentation today is really geared toward the foreign schools and the domestic schools. However, we also know that we have the servicers GAs and third-party servicers and PCAs. The list goes on.

Two different distribution paths. We're reaching out to each one of our guarantee agencies, GAs, and third-party servicers and asking them the very same question that we're asking the DPA. How many people do you have on your systems, what systems are they going to. We're gonna send the third-party servicer their tokens.

Likewise we're doing the same tokens that we're gonna be sending to you. The same token. It doesn't matter. The key thing is when we ask you for that attestation that we need a quick response. We need you to come back and say, "Yep. Steve, this is how many tokens we have."

Alright. So attestation. You've told me ten people. I send you 12 tokens. Each person registers their own token, correct? Yes. No. Right. Okay. Got it. If you off-board someone, if someone leaves we need to actually retrieve the token. It's a government asset. Treat it just like you would if someone leaves, you ask back for the keys to the front door, right. You ask back for their ID badge. Ask back for the token.

You then send an e-mail back to us or when you decouple or deactivate their user ID as you normally would, we're not changing that process. Just however you off-board somebody, continue the same thing. Right now, it's a manual process to decouple that serial number and the name. Remember before we had Jamie over here. We asked her for her name and put her serial number? We will decouple that so that token can be reused again.

So am I sending you more tokens than you need? Yes. Am I gonna send you a lot? No. Alright. There is the cost of the tokens. Not to you, but there is a $20.00 cost to the tokens.

Please, I do not wanna go through the challenges of having to go create a process to charge people for the tokens. We need to make sure that we are good stewards of not only our data, but also the tokens. Put it on your key ring. Have your team keep it on their key ring.

So what we're looking at now are some of the next steps. Portions of my team have been working with our developers and testers and the contractors identifying who's on our systems in three different environments. Now this is really for the GAs and the servicers.

When we say the three different environments, we're talking about test, development and then production. So that's another path. We need to make sure that all those folks are ring fenced and we get them tokens. That's what our team is working on independently. Different path. Once again, we're trying to make sure that everyone has a token.

Once we identify who they are, we're gonna give them what? The training. You guys just did the training. You just saw it so I'm one up on you.

Externally. This is where I need your help. It's that attestation. Reaching out to the primary destination point administrator, making sure that we have all the people that are at your school that you have on a list that we know how many tokens to send you.

Now here's an interesting challenge that we have. The COD security administrator and the DPA aren't always the same person. We need you guys to make sure you communicate so as I reach out to the primary DPA, I'm also asking the question, "Who is using COD?" We need to make sure that they're pulled in as well. Can we do that? Alright. 'Cause I wanna send a package one time with all the tokens you guys need.

That is the extent of our presentation. Questions.

Audience: *[Off mic]* I'm a third-party servicer. _____ different focus for COD users and FAs or _____ _____ _____ the token for both.

Steve Burke: That's a great question. Very good question. It's one token per person regardless of the system. Excellent. No worries, guys. Are there any other – yes.

Audience: *[Off mic]* When a person leaves, we have a staff member that is employed _____. _____ deactivate their –

Steve Burke: Well the token's never deactivated. We'll just decouple it. Tell us that that person's no longer working on your behalf. We'll decouple it. You retain the token. Pull it out for the next person that comes in. Another question over here. I'm sorry.

Audience: *[Off mic]*Are those tokens battery operated?

Steve Burke: Yes. Yes. Yes, they are. They're battery. It's five years. Now what are we gonna be doing in five years? Not this. Not this. No, no, no.

Audience: *[Off mic]*_____ _____ put new batteries in.

Steve Burke: No. I'm so glad, but that's another question that came up. At that point, we'll more than likely be using a soft token or some other technology at that point, but that's a very good question. Thank you. Another one. Yes.

Audience: *[Off mic]* Sometimes when I'm logging into one of those systems I mess up my password and I get the failure. So at that point, do I press it to get another one of those number?

Steve Burke: Sure. You can push the button all day long. But she _____ a very good point. Not all two-factor tokens work the same way.

Some of them reach out to a server constantly and you have to ping, ping, ping and talk to it.

We chose a different architecture. Remember at the very beginning we had those two yellow bars? We sync that serial number up and said, "Start here" for you. So you could push that thing till the cows come home and it'll still work when you come back to the office. Yes, sir.

Audience: *[Off mic]* _____ _____ you said you were gonna send us I guess a little bit of extra tokens than we actually need. Then let's say we need more. Is there a process of e-mailing you or him?

Steve Burke: It won't be Jim. He's already told me that part. It'll be TFA_communications. Now you guys are gonna see more information on IFAP about this. You're gonna have a lot more information on IFAP. Please, we understand that it's a methodical process in the rollouts. Some of you guys won't get your tokens till Q4 of next year. That's okay.

In about 20 days on the COD web page, you will see a link very similar to what we see here on this screen here. Remember I said that register maintain token? That will appear on COD. Don't worry about it if you don't have your token. Continue on with your regular course of work.

My team will reach out to you in advance and say, "Okay, now it's time to register your token." Yes, sir.

Audience: *[Off mic]* Do you always register your token on FSA _____ 'cause I have some people who _____ COD access.

Steve Burke: I'm glad you brought that up. Two systems. Actually the way to look at it, you have to register your token twice. Once in CPSFA access, everything in the Ames world on that side and then our friends of COD.

The two systems were architected differently at different times for different purposes. We tried to look and see how we could do it one joined, but it would not work for us at this time. So, yes, you do have to register your token in two environments. Yes, sir.

Audience: *[Off mic]* We use the _____ client _____ for automating _____ trials back and forth. How are those accounts gonna be impacted by this? There is no person logging into them. It's scripts.

Steve Burke: Machine to machine is not involved. It's when that person logs into the TD client at the very beginning when you start the session that you put your user name, your TG number and what school or where I'm going. That's where you'll see that new field appear and that'll be in February.

Audience: *[Off mic]* So for logging into the SAID mailbox, just the TG number and password. It's not really a person _____. We have multiple IT people that login to that _____ check the mailbox and all that. Is that _____ _____ be exempt from this?

Steve Burke: No. Come February you'll see another one-time password. It starts at the very beginning with that login. That's what's gonna happen in February.

Audience: *[Off mic]* So because we have multiple users though that use that account, _____ _____ _____ back and forth?

Steve Burke: No, no. One token, one person. No. One token per – very good though. That's one of the challenges with our systems. They were built at different times with different purposes and different objectives. The key is it's one token per person. When you login with the user name, we can associate that token with you.

Audience: *[Off mic]* Supposed to get more than one token with one user?

Steve Burke: We'll be able to do that. The whole SAIG piece is very interesting, but our team is on that. We got it covered. Yes.

Audience: *[Off mic]* _____ _____ _____ addressing this question _____. In those two cases where you have one individual that works at more than one institution, I'm wondering if you started addressing _____ got the last Will that person have a token specific for the institution, each of those institutions where they work?

Steve Burke: No. One token. On the back end. We're gonna do it all on the back end to be able to associate specifically for the servicers environment because we know the servicers – let's say an example would be FIA, one of our GAs. If I ask Temple University for their DPA and then I ask Penn State for their DPA and ask Drexel, I would wind up with the same person three times and I would in theory would give them three times if I asked from the schools.

However, I'm going the other way around. I'm reaching out to FIA and saying, "How many people on your payroll and where do they go?" I send them the tokens so it all matches at the other end. So it's one token per person regardless of how many systems that you're accessing. Yes.

Audience: *[Off mic]* From the PD client software that's done without a human, I mean a program, you said there would be no impact.

Steve Burke: Right. From machine to machine, there's no impact.

Audience: Got it.

Steve Burke: This is all about the login and identifying who you are and making sure who you are at the very beginning. Yes.

Audience: *[Off mic]* You indicated that some states were gonna be receiving _____ by the end of this month. Have you already sent the e-mails to _____ --?

Steve Burke: We're going through the attestation now. We started some of the schools already. You see how quick it is. So we just wanna make sure that we have the right names and the right person and we have to have it done by December 31st. Now we all know that school's gonna be shutting down over the holidays. Got that covered. It's only 2,600 people.

When you look at we've done over almost 10,000 tokens now, I think we can make it happen, but I can only do it with you guys' help. Yes.

Audience: *[Off mic]* What is the office desk number? You said it. I didn't hear it.

Steve Burke: No, there is not a phone number. We want everything to come back through the – no, no. I'm serious. TFA_communications. I'm sorry.

[Crosstalk]

Steve Burke: Where you sit. Where you sit. Where your office is. If I wanted to call you during 8 to 5 business hours, where would it be?

Audience: Phone number.

Steve Burke: Phone number. Yes. Good point. Hey Barbara, we gotta change the training, Barbara. We gotta change the training. Very good. That's good. Thank you. Ya' know what? A couple more questions. Yes. I'm sorry.

Audience: *[Off mic]* You said right now if we login to COD since we don't all have tokens, don't worry about the authentication when it appears, but I'm assuming that the plans where at some point where you can't login unless you authenticate your token.

Steve Burke: Yes. What's going to happen at that point, there'll be multiple communications not only through IFAP, but directly with the DPA and the COD security administrator letting you know, okay, the gate's gonna close. The gate's gonna close.

That's why we also gave you those extra few tokens. So the key is attestation and then to make sure that you get those tokens out to your teams.

Audience: *[Off mic]* So is that per school then or is that a copy for everybody?

Steve Burke: The way it works on COD is we're doing it based upon schools, OPID.

Audience: *[Off mic]* So based on when we should have done the process, then it'll be posted for us.

Steve Burke: You'll be communicated ad nauseum from my team. Yes. At no time, and it's critical, we do not wanna stop anyone from being able to do their work. That's why it's a methodical staged roll out. Yes.

Audience: *[Off mic]* _____ person who has a token _____ _____ _____ _____.

Steve Burke: The way we want you to do that if that person's no longer employed by you, you pull that token back. They will get a new token where they go to the new location because when I send these tokens to you that's creating a chain of custody. Then I'm gonna be able to come back and say, "Where are these tokens?" at some point. You're gonna tell me these five people and the other two in the drawer.

Audience: *[Off mic]* _____ _____ _____ _____ _____.

Steve Burke: Yes. We decouple it and you can recycle it, yes.

Audience: *[Off mic]* I have multiple OPID in multiple states. Is it possible because they're in multiple groups _____ _____ _____ could I move one up or one down? _____ _____ --

Steve Burke: That's a great, great question and I love that. The question has to do with I have schools in multiple OPIDs in multiple states. We are starting with the parent OPID because remember that's the – how shall I put it. The participation management agreement says who that DPA is and then it cascades down. So that's where we're gonna start at that spot.

Now, if there are other people in other states, yeah, we definitely wanna get them their tokens and see if we can work that in the process, but we're gonna start with the primary DPA and cascade down. Very much the same way we did with what I call the DeVry model. We went to one spot and then Barbara and her team disseminated them out. Yes, ma'am.

Audience: *[Off mic]* _____ _____ SAIG. We have generic login for people in our office who use that. So how is it gonna work now with _____ getting tokens?

Steve Burke: That will be changing in the future. The way the logins, that part of it. What happens now with SAIG is multiple people can login. Let me put it this way. The key is that we need to make sure that we have one person, one login, that one token. When we give you that token you'll still be able to come through right now on that portion.

In the future there's going to be a point where it's only one login per user, even in SAIG and some more encryption, but for right now – well come February you'll see that piece when we have that one-time password, you'll still see you on the back end of it. Did I answer your question correctly?

Audience: *[Off mic]* No.

Steve Burke: Okay.

Audience: *[Off mic]* I have my own login, my own _____ _____, my own _____ _____ _____. Three other people in our office have their own, but we have a general login or general account for staff. So all four of us share that. All four of us share the password.

So now if I go into SAIG and I use my _____ login, what token am I using to get at it because somebody else in my office is also gonna go in on that same day with that generic login and try to get in _____ _____ transmission?

Jim McMahon?: *[Off mic]* I wish I could tell you. I need to go back and talk to _____ _____ _____ exactly how that works. I know _____ _____, but I _____ _____ _____. I don't _____ _____. So that's something _____ _____ _____.

Audience: *[Off mic]* If I may interrupt, _____ _____ my boss is the _____ and I use _____ _____ _____ allowed me to use it. When I logged in once and I talked to _____ they said _____ setup as a second _____ DPA. So I'm already thinking that anybody who uses the SAIG should be setup as a secondary. I'm assuming then you would _____ --

Audience: *[Off mic]* _____ _____ clerical staff to be secondary DPAs.

?: Yeah. Right now. Understood. Yeah.

Audience: *[Off mic]* Just a follow-up to the _____ counts. We have multiple campuses so we have multiple generic logins. So, one token for multiple _____ login.

Steve Burke: One token per person. Token is per person.

Jim McMahon: I think the simple answer is simply that we're looking at the – and I'm gonna say web-based. I know SAIG is web-based, but primarily internet based application access right now. So we're not as much focused on that SAIG – and I still think of _____, interaction. But we'll get a clarification out.

Steve Burke: Yes.

Audience: *[Off mic]* State agencies, will they receive their key fobs with schools or _____ agencies?

Steve Burke: Each agency. We're reaching out to like FIA, we're reaching out to different state agencies in our systems.

Audience: *[Off mic]* I'm from Maryland. So you're saying Marylanders are going to receive theirs by the end of December. Should I expect one _____ state agency then?

Steve Burke: Yes. Yes, sir.

Audience: *[Off mic]* _____ _____ _____ _____ systems. Will you have _____ single sign on _____ _____ _____?

Steve Burke: Two-factor authentication is not single sign on. Single sign on is coming, but when, I can't speak to that one. Do you have an update on that?

Jim McMahon: No. We've been talking about single sign on forever, right. So I'm not gonna try to tell you it's coming soon, but obvious it's on our list. It's something we're working towards and with the increased focus on the security portion of authentication, we are dedicating more time and resources around that. So it's better looking in terms of us being able to accomplish that some time.

Steve Burke: Do you have a question?

Audience: *[Off mic]* _____ _____ _____ _____. How do I have access and numbers? I usually _____ _____ access and _____ _____ one token?

Steve Burke: That's correct. One token.

Audience: *[Off mic]* _____ _____ _____ _____.

Steve Burke: Yes.

Audience: *[Off mic]* Could you repeat the question?

Steve Burke: She accesses multiple systems for multiple states. It's one token per person regardless of where you traverse. One token per person. Well, ya' know what? Because you guys are here on Friday, this has been one of our better sessions. We thank you very much, but because you guys are here, we actually have a book for you. Now we are not endorsing this.

In all due seriousness, we are not endorsing the book, but our friends at Symantec, they have a great publication. It's called *Cyber Security for Dummies*. Please. There's a handful of them in the back, but we ask you to only take one per company. Thank you very much and we look forward to speaking with you. *[Applause]*