Project Completed by:

VZP DIGITAL

EDUCAUSE
Industry and Campus: How to Prepare for and Ace Your GLBA Audit
Tuesday, August 25, 2020
1:00PM – 2:00PM Eastern
Industry and Campus: How to Prepare for and Ace Your GLBA Audit
Tuesday, August 25, 2020

>> We will get started in just a moment. Stan if you can go ahead and connect your webcam for us?

>> Okay. There you go.

>> Thank you so much everybody. We will be getting started in just one moment.

>> Welcome to today's "Industry and Campus webinar: How to Prepare for and Ace Your GLBA Audit. I'll be your moderator for today. I'll introduce them in just a moment. Let me give a brief -- our presenter slides are showing in the presentation window which is the largest on the screen. You can use the chat to make comments, share resources or pose questions for presenters. We will hold Q&A until the end of the presentation. We encourage you to type your questions in the chat throughout the webinar. If you have audio issues click on the link in the lower left hand corner. Clicking in the top right corner where a drop-down menu will appear. The recording and slides will be archived later today. Thank you everyone for joining us today. We are so honored to have GreyCastle to be an EDUCAUSE partner. Stan is an information and security with 30 years of experience including higher education. Stan works on solving real world problems in security areas. Thank you again for joining us. With that let's begin today's webinar. Stan I'm going to pass it over to you.

>> Thank you very much. I do appreciate it. Thank you so much to EDUCAUSE for allowing GreyCastle to be an EDUCAUSE partner. We are truly honored. All of my attendees have shown up today thank you so much for taking time for this webinar. I owe it to you. I'm going to do my best for you to make sure the content is highly relevant and useful to you. That's my goal. At the end of the presentation you tell me how I did. Today we are going to talk about three areas of GLBA. I like to keep things simple. We are going to talk about what it is that GLBA asks you to do. We will tell you what portion they are asking you to be upon your common federal audit objectives. It is not the full scope of what GLBA is. Lastly, I'm going to give you a few tips and tricks on how to provide evidence how your audit will go more smoothly as you get up to plate and go up to bat there. I did want to caveat up front for those of you in the know and those of you that aren't in the know. GLBA has recently as of March 2019 expanded greatly expanded the scope of what they think educational institutions need to be held to. What I'm going to be talking about today is what is currently in scope. Not what is in scope for the future. We don't know how big that compliance mandate will be in the future. I can tell you that the propose March 2019 -- that proposed set is enormous compared to what we have to talk about today. EDUCAUSE has
valiantly representing you in higher ed to make sure that set gets sized down and right sized so educational institutions won't be choked or overwhelmed by that new GLBA. I do want you to know there is change coming. We don't know how big it will be. Only the FTC will be able to tell us that. All right, so if we could bring up the poll. I just want to ask some questions here.

You can respond to the poll. We will see how you are doing. Where are you in your GLBA journey? Is it scheduled and you are not preparing for it. It is scheduled, you have it or no vote. If you don't want to vote don't vote. Be that way. We have the highest percentage the audit not being scheduled yet. For many of you that is why you are here in this presentation. You want to figure out what to do before that gets scheduled. All right. Jamie, I think we can close that one out. Thank you. All right, let's drop right into understanding the obligation. I am not a lawyer. I can't give you legal advice. I'm not an accountant and I don't do audit for a living. I'm going to talk a lot about what this law actually means and the perspective I'm going to give you is the perspective the layman in security not that lawyer or that accountant. So my perspective is unique and I'm telling it like I see it. So, the Graham-Leach Bliley Act or GLBA as we know it has been in effect since May 2002. If you don't know much about GLBA it is enforced by multiple agencies across the federal government. The Federal Trade Commission is the one that oversees higher ed. Within this GLBA act there are three elements to it. One they call pretexting. I'm not going to talk much about pretexting. If you want to learn more about it Google GLBA pretexting. You don't need to worry about what we are talking about here. The privacy rule which we will be talking about in a minute has been downsized. What we will talk about today is the safeguards rule. Clicking on the wrong thing here. So GLBA applies to higher ed. Why? GLBA isn't that a banking thing? A financial institution thing? When you signed your Program Participation Agreement back in 2015. There is fine print in that that you are going to uphold that set of security privacy of GLBA. That's why higher ed institutions are dragged into it. You are gathering pretty much all of the same information when people ask for loans. Maybe more in some cases. It is a lot of financial information. You owe it to your consumers, your students and their parents. That's why FTC is involved. That's why you are dragged in. So good news. The privacy rules have been somewhat downsized. If you are upholding FERPA and you are compliant with FERPA then you are doing privacy for GLBA. That's the nutshell that you need to encapsulate. A lot of these tie directly to the legal rules and regulations. Some of them tie to our partner EDUCAUSE who does a tremendous job on reporting on these legal issues. So what is this PPA safeguards? Essentially three objectives. It is very boiled down. First of all, insure customer records and information is there. You need to make sure that things aren't going to be disclosed when they shouldn't be and that that information is not going to be modified. That is the confidentiality integrity. Don't give it to the wrong people and make sure it doesn't get hacked and modified. You need to protect against any anticipated threats or hazards to the security of the customer data. Those are big words. What in the world is an anticipated threat? That is something we will talk about when we talk about risk assessment. You need to protect those anticipated threats. Even though you are not anticipating any threats right now. Those threats are out there. You also need to protect against unauthorized access which could result in substantial harm or inconvenience to the customers. That's what they are trying to do. In order to do this, they said higher institutions develop and maintain a comprehensive security program that is written in one or more accessible parts and contains administrative, technical, and physical safeguards that are appropriate to the institution size and complexity. Just because a safeguard exists out there. Maybe a bank is doing that doesn't mean
that it is necessary and appropriate to all institutions of higher ed. You need to determine what is appropriate within your institution. One of the purposes of this written information security program is it gives you the opportunity to say this is what is appropriate. There are well -- I'm not going to say well-defined but well-used guidelines in terms what is a good written information security program. If you want to look at a great example go Google state of Massachusetts CMR201. That is C as commonwealth 201. The first of the union of the state saying here is what you should be doing. If you don't have it in writing, go find one of those on the web. My caution to me don't go grab any document out there and say here is my written information security program. It may be more expansive than what you need in higher ed. The idea behind GLBA is you get to make some of the decisions how to size it down so it fits your program. Okay, so, we are going to talk about what this audit covers. This is my best attempt of a picture of an auditor. In July of 2019 the FDC came out with audit objectives. It has been around for years it just never contain objectives that were explicit to higher ed. Now it does. They came out with that in July of 2019. All right, they don't cover the entire security program as I mentioned a moment ago. And essentially what those objectives are they are going to check to make sure that the institution has named someone or a team of someone to coordinate its information security program. Right? Coordinate is an interesting word. It means that person is not doing it all. Information security is a huge topic. You cannot realistically expect one person in your institution can overwhelming do all the work to keep your institution secure. It is a team effort. Name that person who will coordinate that program. You need to conduct a risk assessment covering employee training and management that works in information security. Those are a few of the topics that GLBA mentions. The reality is to do a good risk assessment you will cover a lot more topics than just those. Information security is not a check box. You don't get to say am I secure, yes or no. It is all of these angles at which to view this thing before you know what your security posture is. So GLBA does require that you done a risk assessment. If you don't have a risk assessment or your risk assessment doesn't look like the real risk assessment you probably will not fare well on the objective. And lastly deferred objective now that you have done your risk assessment you implement safeguards identify risks in those areas. What do we mean by that? What is a safeguard? Typically, we call these controls. They are typically a pretty well written statement. This is exactly how you are going to carry out. Not at the procedural level in some ways you can say what you are going to do. What does that control objective? Maybe a little bit in scope of that objective. So the safeguards, what this is saying, based on my risk, I will figure out what safeguards are appropriate for my program. You can't come up with a list of zero safeguards. You have to do something and the auditors want to check. They want to know and understand that you thought through what those safeguards could be and maybe some of them rejected. It doesn't apply at the university here. So I do a fair amount in the military as well. In the military we have ID cards. My card has a 509 certificate all embedded it. You plug that into special port and everything unlocks for you. That is probably not appropriate in a college campus. The point is there is a whole spectrum what you can go after. It is up to you to get the right safeguards in place. So generally speaking, that is the three objectives. Here is guide to more to than just survival. I don't want you to just to pass your audit. I want you to be secure. I filled out the application for my son. I really will not be happy if that information goes out there and gets hacked. As a parent, as a customer if you will of higher ed. I want my data to be kept secure. That's why I'm going down this path I don't just want to be auditable, I want you to be secure. Let's talk more about how does this GLBA thing work. The obligations they have
for you exceed the audit. The actual common federal regulation or common federal registry. I
told you I wasn't a lawyer. There are various elements that cover five actions for the program.
Number one, you are going to designate that employee or employees to coordinate the program.
It does not say they cannot have outside help. They can. Very often we find that higher ed
institutions don't have a big stack of security folks they can throw on this problem and make it go
away. They need outside help. You need to have an employee or employees to coordinate that
program. You need to identify those reasonably those internal and external risks. You need to
design and implement your safeguards. What is missing here? I said five. Can you count?
Number four, oversee your service providers. What is a service provider? So, within GLBA
there is a pretty good definition of service providers. Let me boil that down. A service provider is
some organization, company, or individual that is going to have access to the financial data that
you are going to be receiving from your students and their parents. Service provider could be
hosted in the cloud. It might be black board. Hopefully, you will not be putting financial
information on a black board. There are a number of things that will constitute a relationship
with a service provider. This isn't a get out of jail free card. You are still accountable for that
information. So what do I do about it? You oversee banner. How do I oversee it? They are huge.
Number one when you select the vendor you got to make sure that vendor is actually worthy
giving your data to before you give them the data. Number two, you got to make sure they
continue to maintain that worthiness. Those are the two basic steps. We can get into that in a lot
of detail in a lot of conversation. For now, that's what I'm going to leave with you. And lastly,
number five, you need to adjust the institutions security program considering the results security
assessment. Put something forward, you test it. Is my test giving me good results? If not, make it
better. Find out where it works and find out where it doesn't work. There is a whole field of
information security that we call security assessment. Lots of security assessments that can go
on. Risk assessment is one way. How are you doing? Are you getting fewer and fewer risks? Are
they getting less severe overtime? What am I doing in my program? All right, let's take these.
We will take the five I talked quite a bit on them. We will go quick through these sections. I will
walk through those elements. Required you got an appointed employer or employees. GLBA
does not -- I'm going to insert the word currently require a CISO. I will tell you March 2019 is
pretty close to saying you have to have a CISO. It is not quite there but it is getting there. That is
the future GLBA that they put out for comment in March of 2019. At present, you don't currently
need a CISO but you need an employee or employees. These are many bullets of warning to you.
You better make sure the employee that receives that program has number one an understanding
of the business, your business as well as security and they need a matter of law here. I have
clients do have legal counsel. They need to know and understand how to look things up. Don't
take people's word for it. Go back to the books and say what I'm I required to do? Sufficient time
to managing the program. If you don't have time to manage a security program, it is not getting
done. So make sure they have confidence, make sure they have time. Confidence by the way is
going to be quite potentially part of that March 2019 assistance. You have to prove the person
you put in charge is competent. Risk assessment. We are moving on. This is number two out of
the five. Risk assessment, this is what is required. Not going to talk that in great detail. I'm going
to give you my cliff notes on it. Number one determine your vulnerables. My suggestion use a
controlled framework. What is a controlled framework? It is a set of security standards put out
by the federal government. The NIST800-171 and the NIST800-53. Came out of the federal
government entire to not choke military sub tractors with 800-53. It was meant for federal
agencies. 800-171 addresses availability. The federal government doesn't care that much if you can't get to your data. You should care about it. So, my assertion even if you use 800-171 make sure whether or not you continuously get access to the data you need. There are many other security frameworks out there. You could do SIS top 20. There is a bunch of control frameworks. These are the two I recommend you think about. So that framework is going to give you that yardstick. That's the way I think of security standards for framework. Here is my yardstick. How do you measure up on it? What you didn't measure up that could be gaps which might in your case represent vulnerabilities. You don't have to comply with it you are going to get a good feeling of broad spectrum of security where are my gaps. As well you need to understand the threats that might exploit those vulnerabilities. A risk simply states is a pair threat in vulnerability. If you have a vulnerability but no known threat, then it probably isn't a risk. It doesn't mean you have a vulnerability. That's part of the value in you going through and choosing appropriate safeguards. All right. So another word of advice for you don't higher someone who can't speak English to you. Security is a world of three letter acronym this acronym the other. I tried not to use a lot of acronym today. I through GLBA at you. I through NIST at you. That's about as deep I'm going to get on acronym. If you can't find a security assessor who can speak to you in plain English, how are you going to know they even found. Make sure they can speak as well. It is important element. All right, create a road map for action. Why do we assess risk? Assessing risk will tell us what we need to do. It will tell us a priority order to go after addressing those risks. It will tell us something about how much do we need to address before it gets good enough. I'm not going to cover risk management in huge detail here. Assessment is the front end of risk management. Risk management is a closed cycle process. Do the assessment. If you don't have the security road map, how do you know what you are going to fix? Are you just shooting blanks? Are you going down the right path here and knocking down the right risks and doing it the right way? Information safeguards is number three element here. For information safeguards here is what GLBA requires. So explicitly they call it technical and physical safeguards. If you leave your data center unblocked that might be a problem. Some of them will walk off. So you got to specify across all of those categories before you get a good feeling on safeguards. 800-53. I'm not using an acronym. Both highly recommended control frameworks for higher ed. 800-53 can be a little bit big, a little bit alarming. In some of your cases if you are new at this you may not want to go in that 800-53. As we get down here toward the end of this presentation, I'm going to give you that how do you collect your evidence. This that I'm going to show you will help you with a template. Overseers, service providers. There is the definition of service provider. They be selected through reasonable steps to make sure they maintain appropriate safeguard. What are reasonable steps? It depends. Good information security folk can help you figure out how to do vendor management. Vendor risk assessments. EDUCAUSE has a tremendous tool. Go grab the HECVAT. It is tailored maybe slanted toward cloud base providers. There may be augmentation
of HECVAT. All right and lastly contracted in a manner that forces maintenance of a safeguard. What does that mean? I'm going to give you a tip that one of my legal counsels gave me one time. They talked about being careful about putting a clause in every contract that says we reserve the right to audit. If you reserve the right to audit your provider. A lot of them are going to say no. We are not just going to accept that. If they do accept it and then you don't audit them. You have made your situation less tenable. Why? You had the right audit. If there is a problem you lose the data they are going to come back to you they were comfortable with our controls and process. They never audited. Be careful with that one. Make sure your contract has some important clauses. One might be, you as a provider agree to uphold the clauses of GLBA. That's a good one. What if they got credit card data? You as a provider must uphold the data security standard. Another good one. Lots of little clauses can go into a standard security addendum which you attach to the contract. That gives you good force to get them what they are supposed to do. All right, I think this is our number five that they are requiring you. Maintain the information security program. Here is what GLBA says about it. Testing and monitoring. Material changes or business arrangements or any circumstances that you know or have reason to know may have a material impact on your information security program. Things change. What are you going to do about it? Either hackers got smarter or you added 57 new servers in the data center or maybe you moved everything up to the cloud. Whatever the circumstances. Things change. Make sure you maintain your program. Continue to review it and go through and make sure you are doing the right thing. Generally speaking, this is generally speaking. Look for new vulnerabilities. Look planned and unplanned changes in your environment. Look for changes in that threat landscape. Take a look at those threats that are out there. In some form of cyberthreat intelligence. There are organizations out there. There is a number of free ones if you Google them. Grab that data. Read it every now and then. We don't want to know it, but if you don't know it how are you going to know if the threats change? How will you know if some of those threats are applicable to your environment and you are not doing anything about it? So go get educated on them. So how do you survive the audit? We talked about what it is that the program requires and what the audit objectives are going to be. Documentation is a key. I know there are organizations that are in the CPA business. I thank you for joining us. Let me give you my layman terms in here. If I bring an auditor in. They are going to ask me questions. Do you do this? Yeah, I do that. What is the next thing they ask? Show me the evidence. Where is your evidence? Can you prove you have a security program? Can you prove you have proper security controls that you selected that are in place? Can you prove that you are doing a risk assessment? Can you prove that you are doing risk management? Where is the evidence? So this little one-page sheet I'm going to animate it out here for you. You are going to have a written information security program. We talked about that. Your written information security program or written security program had better say what it is that you actually do, not what is best practice, but what do you do? Accountability for implementing a program. You need to be able to show that. Who owns the program? It has to be an employee or employees. Are you doing a risk assessment? It also better provides a written report at the end of it from whoever does that risk assessment. Where is your evidence? The safeguards, what you list as safeguards. Here is a sample spreadsheet which we are going to walk you through. This is -- hopefully you can see this. I know it may be a little bit small. In my screen I can't see it too well. On the left-hand side you will see the headings and sub items that are part of the regulations that you are trying to comply with. In the middle column here under description, we are talking about explicit activities that
the college or university is doing to meet those objectives. Now, not everything you do will apply just to one objective or one element I should say of regulation. Some of those things can appear in multiple lines. Some of them are soft and squishy. Your job is not to provide concrete evidence across the board but to give them that broad look at how I'm doing on this. Here are the things I'm doing. The status column should provide, you know, is it something in progress? Did I finish it? Or is it yet to be done? So animating this out. Reference to regulation. Number two, show what you are doing on that. Number three, give a status with dates. It is really pretty simple. This will help organize your evidence. This is not all the evidence you need. That's what I'm trying to tell you. You will probably need more evidence than this to pass your audit. I mention that risk assessment report. I mentioned your security controls. So in an approach like this hopefully will get you organized and keep you a little more organized. Believe it or not I finished with my drawing. Hopeful I didn't put anyone asleep. Here are three things I want you to walk away with. You don't have a choice with GLBA. You signed that PPA. GLBA is a bit vague but expansive. It is good and it is bad. I worked in credit card security. Credit card security is restrictive. It is the same formula for everyone that ever touches a credit card. One of the beauties you get to look at it. You get to say this one does not apply to or organization because we don't do whatever it is that makes you not applicable in that category. It is not a question of whether or not you like the safeguard. It is whether or not it applies in your business. And then lastly, I think I hit this item already. The common federal audit will cover only a subset of GLBA. Don't flash forward to 2021 because we don't know what is going on there yet. But for 2020, that's the story. I finished. Questions for all of you. I see a big list of questions. I'm hoping that Nina can get back on with me.

>> How are you doing?

>> Doing well.

>> We have great conversation going on in this chat. We have a lot of questions. I'm going to head right to them. Brandon asked one of our vendors said this to us. GLBA doesn't affect colleges with respect of federal loan since they are handled through the department of education. How do you validate that statement?

>> I really have to parse this question. Thank you, Brandon. It sounds like your vendor is telling you that colleges don't have to be under GLBA. I guess what I encourage you to do think about it this way. Are you accepting Title IV funds? You had to sign that 2015 participation agreement. That binds you to be under GLBA. You are not a bank. You are not under the full GLBA elements but the five elements I listed are very explicit in GLBA with respect to higher ed. Hopefully that answers the question Brandon.

>> He just commented in the chat saying asked them what they were going to comply with GLBA.

>> So it sounds like your question is more -- the vendor saying they don't have to comply. And you are asking them what are they going to do with respect to GLBA? My advice there going back to putting in place a set of addendums. The vendor will be holding to you not to the
department of Ed or to FTC. They will be beholden with you. So you got to make sure it is in the contract language. That's why I recommend a fairly security addendum. I'd make sure I have a clause in there that says that they will uphold any portion of GLBA that you are required to uphold. If you have to have a security -- I want my vendor to. I'm done, Nina.

>> That's okay. Another question we have from Rick. Does a risk assessment need to be conducted from external group or internal? How often do you need to be doing risk assessments?

>> Risk assessments does not required to be done by an external organization. If you have people that are competent in risk assessment you are probably fine. I live the idea of external assessor. The reason why I like it if you get people looking at it from different perspectives, they will see different things. Within our company we don't like the same risk assess sore year over year over year because different ones will ask the questions slightly different. They will get a slightly different viewpoint. We are going that 800-53 framework. But every assessor is going to have unique specialties. I had 20-25 years of software development. I'm a weird one when it comes to information security. Most information security folks came through hardware and networking. When they ask questions about software security and how you secure your software develop process many of them miss the nuances that I pick up on. You are not required to. Your second question is how often should you do it? That will be up to you. Generally speaking, a lot of guidelines say once a year is good to go on. If this has never been in your security budget, I recommend that you start, you test it, you see the value of it. You will be required to come up with an intra value with that.

>> And we had just a follow-up question to that. What level does the risk assessment have to be applied?

>> Again, as I look through with risk assessment my personal favorite I'd like to go this 800-53 to give me those broad categories. In an 800-53 there are 18 control families. If you want to see what they are go Google control families and you will find a list of 18. There are things like access control, identity and authentication, awareness training. There are 18 or so of those. It should cover that broad scope.

>> Thank you, Stan. This is more than a comment. Carol commented -- specific risk assessment. They don't accept the high-level risk assessment and want you to know the safeguards over the entire network.

>> Okay, well first of all, to the best of my knowledge there is no such animal as a GLBA risk assessment. It does not have to say it is a GLBA risk assessment. You need to do a risk assessment. Based on those risks you need to look at a control framework and say these are the safeguards that were implementing to drop the level of risks across those. Again, what I would like to do, I'd like to start with a good security framework 800-53. Within that there are hundreds, literally hundreds controls spread across those 18 categories. If you walk through each category you are going to have to get the right people in the room. Got to get the right audience and it takes work. You want each control family and you determine does this apply in our institution? If it does not apply, I document why it does not apply and I say that is not a
safeguard we are going to implement. Does this apply in our institution? I mentioned this during the presentation. You are not asking the question whether or not you like the safeguard or whether or not it will be easy. The question is does it apply given your way of doing business. Hopefully that helps.

>> Thank you, Stan. Gabriel asked what about using the SSIEC cat tool for risk assessment. I have seen that recommended.

>> Used for the federal credit union. And the NCUA and other organization national credit union association and other financial they refer to FFIEC. FFIEC control applies here. Using the cat would be appropriate in this case because we are talking about financial data. It is not technically speaking a risk assessment. It is a control framework. You are still going to have to wrap some kind of risk assessment methodology around use of that framework. What FFIEC gives is more of a maturity model. How are you doing relatively to the overall gap. That tends to speak more of a risk. Remember I mentioned a risk is a threat, vulnerability paired together. I have that gap and this threat exist. What am I going to do about it? Be careful using the FFIEC. It is a wonderful tool. It comes in a spreadsheet. It is super easy to use and self-assess. What you are doing is a gap assessment with a little bit of maturity model at the end. Different than a risk assessment.

>> Thank you, Stan. Another question we have here. Why do you recommend 800-53 when the EDCL recommends 100-171.

>> I kind of covered this for you. To me as I read through it and compare apples to apples. What is missing? It is more of the controls. As far as the federal government is concerned, if you don't lose the data and not subject to the modification you are pretty happy. Just don't lose it. I feel they are missing out on the availability thing. We want to know that our information is available. That's a risk to our institution. So that's why I tend to slant toward that 800-53 rather than pure 171. It isn't that you can't use 171. Don't forgot to use risk to availability. I know those are broad -- it is roughly right.

>> Great. Thank you, Stan. Ben stated are auditors want more than a spreadsheet.

>> It is always their right to ask for evidence. That's spreadsheet is not going to give you a full set of evidence. It is a way of kind of organizing your thoughts and explaining we did this project that goes to that. If you don't document that project, how are you going to show them evidence you did the project. So I use the example of risk assessment. If you do an internal risk assessment this is kind of a risk, that is kind of a risk. You don't write it up in a format that proves to them that you looked at probability and harm with respect to a threat vulnerability pair. You haven't assessed risk. You may have done a gap assessment. If you didn't produce that report that has some key and critical elements, then they are probably going to say not really elements big risk assessment. Let's pick on another one. Access control. Right? It is common practice in every security framework out there to say you should be doing regular access control review. What does that mean? It means go through your active directory. They shouldn't be in there, right? If you do that great. Keep some form of documentation that shows that you do that on a regular basis and as our question asked make sure it shows it within the audit window they are looking
at. If it is a one-year window you don't want to show them evidence doing that eight years ago. Hopefully that helps.

>>> Great. Thank you, Stan. Brandon asked does it have to be organizational or can it be system based?

>>> Again, excellent question. That is one of the things that people are poking at in the comment period against the new GLBA controls. And EDUCAUSE along with another non-profit organization brought this up. The FTC has a pretty broad definition in there what should be going on. They aren't eliminating that in the current definition to only the financial data. When you talk about GLBA specifics. The way I'm interrupting that surrounding our financial data. If you've got information about your dining hall, residence room assignments is that GLBA scope? Not really. That is information about residence fall assignments. I would say that the FTC has no business going after that data and mandating you have safeguards around that. I think you better from a security perspective. I don't want my information hacked. There is security, there is compliance. You can be security and not be compliant. You can be compliant and not be secure. From a GLBA perspective it is easy to get into a scenario can overreach their authority and over audit things. It will be up to you during an audit is to actually be able to push back. To able to say, you ought not to be going into this. All right, folks I'm about out of time here for questions. I apologize to abruptly stop. I'm going to hand to our team of EDUCAUSE. Thank you so much for your time.

>>> Thank you so much, Stan and Nina. If you have any questions you can reach out to GreyCastle. Someone posted the link in the chat and also on the slide there. Slides and resources will be posted you will find that link on the chat. Thank you everyone for joining us today. We appreciate all of your questions and comments in the chat. Before you sign off today please click on the session evaluation link. Your comments are very important to us. Again, this session recording will be posted later today. Please feel free to share that with your colleagues. Finally, please join us for the next campus webinar on September 3rd to hear about optimizing the distance learning experience and virtual classroom. Thank you all again for joining us today.

>>> Thank you.

[ Event concluded ]