Please note: This is a transcription so there may be slight grammatical errors.

Hello and welcome to Revamping Retirement, a podcast brought to you by CAPTRUST, where we explore the opportunities and challenges facing today's retirement plan sponsors and fiduciaries. Our hosts, Jennifer Doss and Scott Matheson, lead the employer-sponsored retirement plan practice at CAPTRUST, one of the largest registered investment advisors in the U.S. and a thought leader in the retirement plan advisory and consulting space. We hope you enjoy Revamping Retirement.

Scott Matheson (00:35):

Welcome to another episode of Revamping Retirement. I'm Scott Matheson, and I'm not joined by Jennifer Doss today. Apparently, she actually needed a month off from talking with me. But fear not, loyal listeners, you will not be subjected to a monologue from me today. I managed to trick … I mean lure … I mean I found two of my very talented colleagues who were excited to join me for today's discussion. That said, welcome to Revamping Retirement, Audrey Wheat and Jon Atchison.

Audrey Wheat (01:04):

Thanks, Scott. Excited to be here.

Jon Atchison (01:06):

Yes, thanks, Scott. Glad to be here, too.

Scott Matheson (01:09):

Well, I'm excited you guys are here as well. But maybe let me tell our listeners why they should be excited that you're here, too. As it turns out, October is National Cryptocurrency Month. The two of you are here to debate which is a better investment, Bitcoin versus Litecoin.

Audrey Wheat (01:27):

That is not what your invite said, and I am more of a Dogecoin girl.

Scott Matheson (01:29):

Okay. I don't even know what that one is. All right, I am kidding. Fair enough. That's not what I told you you were here for. So we will go with the original plan, or plan B, since you guys didn't bite on that, because in addition to October being National Cryptocurrency Month, and of course National Halloween Safety Month, October's actually National Cybersecurity Awareness Month.

As our employer listeners know, or many of them know, probably most of them know actually, understanding and evaluating cybersecurity risks continues to be really a growing part of their responsibilities. Yet … And I'm just going to speak for myself here just in case it does resonate with our listeners, but I often feel woefully undereducated on the broader topics and create resources and training. In come my two guests here.

Jon Atchison joined us at the beginning of 2020 and brought with him to the firm nearly 20 years of experience in systems and IT-specific security related to really the IRA industry, the investment advisory industry, that we are in here at CAPTRUST. Here at CAPTRUST, he actually leads our internal IT security, governance, risk and compliance efforts for our entire firm's IT network.

Audrey Wheat has been with us for seven years now, just shy of seven years. She spent the first two-thirds of her career working on the record keeping side of the retirement industry. Today she is actually a senior leader on our 10-person dedicated vendor analysis team.

So with these two together, I'm super excited for this conversation, because Jon and Audrey have been partnering closely for the past year and a half now to help our plan sponsor clients leverage the expertise Jon and his team have accumulated over the years related to themes around cybersecurity.

Audrey, why don't you get us started here and remind our plan sponsor listeners of their duties related to cybersecurity and how those really shifted last spring, April, I think it was?

Audrey Wheat (03:25):

Sure. So in April 2021, the DOL released three pieces of different guidance. To break them down, the first one was plan sponsor cybersecurity responsibilities and best practices. Then they put out some tips on hiring service providers. Then, finally, they issued some online security tips for participants. So with those three documents, plan sponsors received a lot of information and they looked toward us for help with breaking it down.

So, Jon, you and I have been working together on this since the guidance was released. What does the guidance mean for plan sponsors and why and how should they make it their responsibility?

Jon Atchison (04:10):

Well, broadly speaking, the guidance has presented these tips or best practices, and plan sponsors really should consider them as a minimum baseline of what should be done to identify and address cyber risk in its various forms.

For the second question, while not an explicit framework like the NIST 853 or the CIS-20, or even the ISO 27000, the Department of Labor's guidance serves as a common starting line for all that fall under that particular umbrella. That's the why.

For the how, all entities that fall within that scope can now point to a unified approach in addressing cybersecurity risk, bringing them to the same table and asking the same or very similar questions of themselves and others involved in serving their clients' investment needs. Because the DOL's guidance is a baseline intended to aid plan sponsors in making prudent decisions, this means the industry has a chance to become stronger in the area of protecting client information.

Scott Matheson (05:13):

Well, that sounds important. I also think that you just cracked a first here for us. I don't think we've had any references to ISO on the podcast today, Jon. So well done there.

Jon Atchison (05:25):

Thank you.

Scott Matheson (05:26):

I was thinking to myself, ISO 27000, is that like DOW 30000? Is that what that's like? Not sure that applies. All right. Well, in all seriousness, a year and a half after the DOL's guidance was released that we just talked about. Thanks for breaking it down for us. I'm curious, so maybe Jon, from your perspective, because you've dug in beyond the walls of CAPTRUST into the client realm for us here, I'm wondering how you're seeing plan sponsors evolving approaches, their approaches, to cybersecurity, to IT security, data security, all in, in light of this guidance?

Jon Atchison (06:01):

Well, the good thing here is that the DOL guidance has standardized the approach plain and simple. There's not really a need to have a highly complex or technical knowledge of cybersecurity. Their guidance breaks it down in approachable language that is easy to digest.

CAPTRUST receives consistent inquiries from plan sponsors about how we align to DOL guidance and how we vet record keepers for their consideration. It's really hard to overstate the importance of having a standard approach. These best practices serve as a plumb line, in a matter of speaking, that plan sponsors can use to benchmark against and when they're inquiring of current or prospective fiduciaries and other service providers.

Audrey Wheat (06:45):

So that's a lot of work, that's a lot of responsibility, but the work is never over. So, Jon, in your perspective, what else needs to be done?

Jon Atchison (06:54):

Well, that's a big question. So hopefully by this point in the game, plan sponsors, fiduciaries, and industry service providers have identified their own areas for improvement and acted upon them. Essentially, you find out where your gaps are when you start looking at the DOL guidance.

From my perspective, remaining consistent and diligent in some core areas really come to mind. Cyber insurance, while considered optional for many years, is now seen as a must-have. I would think maybe 10 years ago, selling asteroid insurance would be an easier bet than selling cybersecurity insurance. But as we see with the current threats, it really is necessary.

Also properly understanding your own security posture is only going to aid you in the cyber insurance review process, and promoting your capabilities to a prospective insurer is certainly going to help that cause. They're going to better understand you as a company and better help to assess risk and hopefully get a better rate in the long run.

Review those prospective policies that you're considering. Dig deep into the clauses and search for exclusions of coverage that may not quite satisfy your needs. For instance, insurance carrier …

Jon Atchison (08:03):

May not quite satisfy your needs. For instance, insurance carriers might likely carve out exclusions pertaining to state-sponsored attacks. So for instance, if China or Russia or some other rogue state like North Korea makes a broad attack on the U.S. and your company falls into that net, you may not have coverage from it. So read those policies carefully. It's really, really important to know what you're getting and what you're not getting. And you have to ultimately ask yourself would this be acceptable to your company if you were targeted and breached by a nation state actor? Well of course the answer would be no, I would think.

Another area would be to have a due diligence process when evaluating third-party service providers. Understanding how sensitive data could be shared and how it would be protected by the third party is of utmost importance. Consider using a third-party security assessor to aid in your due diligence efforts. And what is that? That's a company that can scan for vulnerabilities that these third parties may have from a public-facing perspective. What would an attacker likely jump on first? These companies can help you understand what those would be, and often quantify that with a risk score. Finally, finding and partnering with a third party who demonstrates strong cybersecurity practices really should be high on that list. And fundamentally, and I think Audrey, you can relate to this, proper due diligence can help separate those that do from those that do not.

Audrey Wheat (09:30):

Absolutely.

Scott Matheson (09:32):

I'm not going to lie to you, I had to go back while you were talking there and Google plumbline from your earlier answer. Impressive use of it, by the way. Well done there. I'm also wondering if asteroid insurance is a real thing now. So you completely distracted me, which is by way of mention, I'll tell you—

Audrey Wheat (09:48):

Par for the course.

Scott Matheson (09:49):

Yeah, right. I'll just mention that also October is national ADD awareness month, interestingly enough. I don't know anybody with that, but … So real quick, the two of you guys have been partnering together or have partnered together alongside both of your teams to create something that's really robust, yet I think elegant in how easy it is to comprehend. And listen, we always try to be careful not to use our podcast to push our own agenda or come across as salesy by any means, but I really do think that sharing what you've built will be super informative for all of our listeners who are on their own trying to tackle their responsibilities here. And hopefully they can grab some ideas from what you all have done. So that is a backdrop and a qualifier, if you will. Audrey, why don't you tee up a little bit about the process that you guys have built and deliverable and how plan sponsors are consuming that?

Audrey Wheat (10:42):

Yeah, absolutely. So it's obvious that at CAPTRUST we have these wonderful resources as a part of Jon's team for our own cybersecurity, but we wanted to leverage those resources in a way to help our clients. So when the DOL released the guidance last year, we immediately thought, "What can we deliver as an advisor to help our clients understand what their specific record keeper or vendor partner are doing with cybersecurity?" Because they all have a bit of a different approach. So Jon and his team are already experts at vetting the vendors and systems that we at CAPTRUST use on a daily basis, so we should leverage their expertise to help our clients. So Jon, let me shift to you. Can you talk about the analysis that you and your team do and how you've designed this to meet both the DOL's requirements, but also incorporate the latest and best thinking and learnings in the vast landscape of cybersecurity?

Jon Atchison (11:39):

Yeah, you bet. Ultimately, we want to find out if our third parties can walk the talk. We said here in Alabama, you'll find world-famous barbecue in every city. Well, I'm not so sure that's the case. According to who is the barbecue famous? So the same analogy … The same analogy applies to cybersecurity. I think everybody can say that they do something, but how do we really validate that? And when it comes to cybersecurity, this is not an area where we can afford to be wrong. Our due diligence approach seeks to employ best practices, just makes sense for evaluating our third parties. And as available, we evaluate multiple sources of information in the due diligence process, including direct engagement with the third party. I think establishing that line of communication with them is really critical to getting a good outcome.

Ultimately to help these efforts we partner with a third-party security assessor. When I mentioned earlier about scanning the external attack surface of a company, they help us to identify cyber risk that third parties might bring to the table. Through external scans and other methods the platform offers us the ability to start a meaningful conversation on risk, ultimately culminating in a refined view of where material risks might actually exist. And secondly, the third-party assurance documentation, or in other words a SOC report, is a critical piece of the process. And this is that objective third party that we can lean on and they can be the tale of the tape, on somebody's strength in cybersecurity or perhaps their weaknesses. We rely heavily on their opinion, on the SOC audit in terms of opinion, and that SOC report also serves as a great place to have a meaningful conversation with a third party, should there be any findings or items that catch our attention. And so far we've had good conversations.

Scott Matheson (13:31):

So really, when you say you're saying third party generically, but here we're talking a lot about primarily record keepers, right?

Jon Atchison (13:37):

That's right.

Scott Matheson (13:38):

Okay. Well, I am really curious to hear from you about how the record keepers and other vendors are responding to all these requests, but before we go there, we really need to take a quick break and I'm going to kick it over to Mike Webb for our monthly Minute With Mike. This month Mike's actually going to give us a really interesting rundown on an idea that he has. I don't know that he has it, but he definitely has flushed it out here in terms of a unique way, yet simple way, yet really effective way for plan sponsors to monitor the success of their retirement plan vis-a-vis participant engagement. So with that, take it away, Mike.

Mike Webb (14:15):

Thanks, Scott and Audrey. Mike Webb here with another Minute With Mike. In this month's Minute, we'll discuss a less common but highly effective method to measure success in a retirement plan. But before we get to that, I wanted to dedicate this Minute With Mike segment to the memory of my former colleague, Ellie Louder. Ellie taught me more about 403B compliance issues than I probably learned from everyone else combined, and there would almost certainly be no Minute With Mike without her. She was always very supportive of me and she will be greatly missed. Now back to measuring retirement plan success. There are many ways to measure the success of a retirement plan, from simple methods like assessing plan asset growth, average account balance, and voluntary participation percentage metrics, to more complicated approaches, such as monitoring the percentage of participants on track to accumulate enough to successfully retire.

However, there is a question that many plan sponsors fail to ask their record keeper that may be one of the most telling dodges of retirement plan success. And that is how many retirement plan participants have never logged in to their online retirement plan account. In many plans, that number can be shockingly high, and there are a few reasons why it's crucial for plan sponsors to improve this statistic. First, having a large number of participants that do not engage with their plan likely means that the reason that the return on the employer's investment is not paying off as well as it should be. Either participants do not realize the benefit of their retirement benefits or they are just simply not aware of them. Number two, inactive online accounts can make the plan more vulnerable to cybersecurity and traditional fraud risks, as inactive accounts are more likely to see fraud go undetected. Number three, online access …

Mike Webb (16:03):

… detected. Number three, online access generally indicates other success statistics. For example, if participants aren't logging in and the only way to increase or initiate a salary deferral election is online, then it is likely that voluntary participation and deferral percentages are suffering. There's also a sustainability issue from a lack of online engagement. Inactive online accounts mean the plan is probably wasting money on paper transactions. If a participant is never logged in, chances are they have never opted into paperless communication. This paper increases record keeping and administrative expenses for the plan. Plan sponsors who are not tracking this participant login statistic would be wise to start doing so today. For Revamping Retirement, I'm Mike Webb, and this has been your Minute with Mike. Now back to Scott and Audrey.

Scott Matheson (16:53):

All right, thanks Mike. That was a really interesting idea and I'm actually surprised cause I don't hear about it an awful lot, that it doesn't get more chatter. So well done there. Welcome back everybody else to my conversation here on cybersecurity with my colleagues Audrey Wheat and Jon Atchison. Before the break, we were talking about the incredible tool the two of you and your teams have developed to help our plan sponsor clients. And Audrey, such a big part of your job is managing dozens of relationships for our firm with really key record keeping partners on

behalf of all of our clients who entrust us with those responsibilities. I am curious, as I said before we took the break, how are vendors responding to all these requests?

Audrey Wheat (17:33):

Yeah, so in the spirit of partnership, our vendor partners have been extremely receptive to working with us to dig into their practices. One common theme that we've heard is all the vendors emphasize that when they work together, everyone is stronger. So on the other side of the coin, they feel that when one fails or falls, they all fail. So when we meet with the record keepers, they are very excited to show off their offering and help us understand how to best tell their story. So Jon, it might also be helpful for you to share how you are seeing the record keepers change their policies and approaches in response to the DOL guidance and maybe even to the inquiries from plan sponsors and plan advisors alike.

Jon Atchison (18:21):

Yeah, sure thing. So for one, record keepers are posting their responses to DOL guidance on their websites. And this is heartening to see. For the public to go out there and take in the information, I think this provides a level of transparency and it shows alignment with the guidelines that DOL has issued. And I think ultimately the intent is to build trust and it gives people a good point to reference to. They know that record keeper A is doing this really well and they have all this good information.

And I think it just ultimately benefits the participant and plan sponsor. In the long run, record keepers, fiduciaries, and plan sponsors all have that same guidance to benchmark and operate from. And if anything, adopting that standard approach to the topic of cybersecurity has been most helpful in conversations that we have with our key record keeping partners. I think it's fair to say that there is good alignment on what should be done from a cyber perspective. And I really think this goes to fostering shared values in cyber risk management. And I really agree with what you said. When we all work together, everybody really is stronger.

Audrey Wheat (19:25):

Yeah, absolutely. Is there anything you're noticing that they aren't doing or changing that you think needs to be done at this point?

Jon Atchison (19:34):

So I think every record keeper that we work with has every incentive to do it right. I think we all have every incentive to do right by our clients and do right by the roles and responsibilities that are put before us. And so I'd say broadly, don't fall asleep at the wheel. Okay, so we have a good program, you have a good program. What are you going to do to keep it good? To those outside of information security, the topic can be mysterious and exciting. And maybe even conjuring images of battling bad guys who wear hoodies in dark rooms banging away on laptops. Well

that just isn't reality. Yes, the threats are definitely real, but the most important thing in information security is keeping up with the little things and this is how you build and maintain a good program. DOL guidance I think really shines in this area.

Scott Matheson (20:24):

Man, that's so good. Also love the imagery there. Just a phenomenal way of telling stories—

Jon Atchison (20:31):

It's an advertising [inaudible 00:20:33].

Scott Matheson (20:33):

Yeah. Well what you guys have done together here is obviously pretty impressive. Let me shift from maybe away from the plan sponsors directly to how they're working with their participants, their employees that they care so much about. So Jon, I'll start with you here maybe, any additional tips you'd share for most of our listeners who are employers, plan sponsors for things they can be thinking about or implementing to protect their own plan participants and the beneficiaries of these plans from cybersecurity threats?

Jon Atchison (21:02):

Yeah, sure. Sure. So think about when you're researching something you want to buy, you invest time, you start looking up information or reading reviews about the product. Just as an informed consumer makes better purchases, a risk informed participant is really going to position themselves pretty well against common cyber threats such as phishing, identity theft. For plan sponsors, I really think finding ways to present creative and fun opportunities to educate their participants in cyber risk is really key. I think having a good cyber education program is paramount to establishing a good security culture.

Audrey Wheat (21:40):

And we really encourage plan sponsors to communicate to plan participants about their own responsibilities. There is an onus on the participant as well. So basic reminders like register your online account, check into that account ever so often, monitor that account and make sure your contact information is up to date, whether that be through the record keeper or through your employer. Those can really help prevent attacks.

Jon Atchison (22:09):

Yeah, no doubt. And don't forget the importance of using all the security tools available to you. Complex passwords are important. Store them in a secure password vault or in LastPass or another comparable product there. And of course, don't do silly things like write your

passwords on sticky notes and put them on your keyboard. And use multifactor authentication where you can. They're like the seat belt of information security. The seat belts won't prevent you from having a wreck, but they'll certainly keep you alive. Having multifactor authentication on an account prevents over 99% of all attacks against unauthorized access. Think about that. That's really an effective tool.

So enable multifactor authentication where you can and have them send text codes to you or email you access codes as appropriate. Sometimes companies will have soft tokens that will pop up on your phone. That's also an effective tool as well. And this may feel painful, this may feel like, "Why am I burdened by all this technology?" Well believe me, in the short term, the pain is going to pay off in the long run because it pales in comparison to the absolute disruption you will experience if somebody hacks into your account and steals your funds.

Scott Matheson (23:22):

Well that is great. Great advice from both of you. I now know what I'm doing this afternoon, turning on multifactor authentication, tearing up all those sticky notes. Just kidding. I don't have sticky notes Jon, I don't want to get fired over this joke. That was not a good joke. Never mind.

Jon Atchison (23:38):

All good.

Scott Matheson (23:40):

All right. Great job from both of you here today. Great job in what you've built. It is meaningful for all of our plan sponsor clients, but ultimately at the end of the day, most meaningful for the participants whose money is entrusted inside of these plans and who we're all entrusted to do what's in the best interest of. So love that y'all are doing it. That is awesome. As always, we always save the hardest …

Scott Matheson (24:03):

As always, we always save the hardest question for last. And since I have two of you here, I'm going to get to ask you both this. So, surprise on that. I think we gave Jon the heads-up. I'm not sure, Audrey, you got the heads-up. Okay, we're going to go with it. So Jon, I'll start with you in fairness to Audrey, partly because we're the same vintage and are marginally closer to normal retirement age than Audrey is, 20 years or so. Our listeners are definitely curious, as they always are with our guests. What does retirement look like for you, Jon Atchison?

Jon Atchison (24:35):

That's a great question, and I've given some time and thinking about it. I love to fix things and build things, and I love to learn. For years, I joked with my wife and I was going to put one of

those vehicle lifts in our driveway to go full Alabama on us so I can work on our vehicles like the professionals do, right? Well, I don't think my HOA is going to like that idea very much. And despite those car repair ambitions, the thought of learning new skills in this area is really appealing to me. I think just having more time for that. Ultimately, my broader desire is to spend more time with my wife and three children and to find new ways to make the most on this life given to me.

Scott Matheson (25:14):

Well, that's a great ending to that. And as long as you have your plumb line there and you don't fall asleep at the wheel while you're doing this work, you're going to be fine, Jon. Great answer. All right, Audrey, he bought you some time. What does retirement look like for you, Audrey Wheat?

Audrey Wheat (25:32):

Sure. Well, one thing I look forward to most is not receiving those phishing emails from Jon's team, having to pass those. It feels like they come once a week, but hey, I've been getting pretty good, Jon. I don't think I've failed in a very long time.

Scott Matheson (25:48):

Actually, she hasn't wired money to fielding in a long time.

Audrey Wheat (25:55):

But thank you for asking me, Scott. I have worked since I was 14, and I firmly believe that staying active is really the key to a long life and a healthy life. So with that being said, stereotypically, I want to travel as much as I can. I want to help others, and I want to spend time with my loved ones. And then I also do have a pipe dream of. At some point, I do want to be a flight attendant. I just feel like I'm going to do that at some point in my life.

Scott Matheson (26:23):

Oh, this is news.

Audrey Wheat (26:25):

Yeah. Yep. After I retire, I promise.

Scott Matheson (26:28):

Okay. Wow, that I didn't see that one coming. I mean, I've been surprised by a lot of these, but that one, that's a good one. All right, well, you can fly down to Alabama and check out Jon's

garage in the front of his house that his wife's upset with him about and isn't spending all the time he want. It's going to be great guys. You guys are going to great retirements. But the good news for me, the good news for CAPTRUST, the good news for our clients is both of y'all are a long way away from that.

All right, here we go. If you're willing to come back in the future, maybe, we'll see how that's evolved. Maybe air travels now what you want to do in the end, and maybe, Jon, you can just put something, carport out back and take care of the front yard problem you have there. But anyway, I do appreciate you guys coming today, spending time with me. Had a lot of fun talking to you as I always do. Hope our listeners picked up a few extra nuggets there themselves.

I would tell everybody that's out there, check out the show notes for today's episode. We will actually link a few resources in there, some videos we've created, a replay of a webinar that we did, post the Department of Labor, if you need that refresher on summarize many of the tips and topics that Jon and Audrey both discussed here today.

Next month, join us because Jennifer and I are going to be talking, having a really cool conversation on HSAs with Lindsay Barnard, who's actually the product manager on what I'm going to call a revolutionary new HSA platform, designed and launched this year formally by Allegis Technologies. Allegis, if you don't know them, they're a lot behind the scenes, but they are the leading provider of technology-based benefit funding and payment solutions. So you won't want to miss this because HSAs are increasingly growing in popularity, and the intersection between health and wealth, if you will, as we think about the retirement landscape is definitely happening.

So you've done it again, listeners, you've made it to the end of another episode of Revamping Retirement. Congratulations. As always, don't forget to like and subscribe to wherever you get your podcasts and leave us feedback if you have any. On behalf of Audrey Wheat, Jon Atchison, Jennifer Doss, wherever she is, Mike Webb, our sound engineer, Ben Farmer, and our producer, Carol Macauley, I'm Scott Matheson saying, thanks for listening, and we'll talk to you next month.