Please note: This is an AI generated transcription - there may be slight grammatical errors, spelling errors and/or misinterpretation of words.

2024 Fiduciary Training Series, Part 4 Avoiding Scams

Lisa Keith: Hey, welcome to this quarter's fiduciary training webinar. I'm Lisa Keith, the senior manager on our retirement plan consulting team here at CAPTRUST. Today we are going to discuss a topic that has touched everyone at some point, scams. Specifically our focus today will be on scams that target your participants in their retirement account.

The number of bad actors out there continues to grow and retirement accounts are increasingly being targeted due to the large amounts of money available within those accounts. So what can plan sponsors do to protect their participants? We have assembled a great panel today that will talk about current areas of concern, the latest DOL guidance regarding cybersecurity, some interesting cases, and then some practical steps that will assist the plan sponsors with this important responsibility.

So, let's go ahead and get started with some introductions. Cindy Landy, So Cindy is a member with Brown Winnick and she serves on the firm's executive committee and leads the firm's employee benefits, practice group. She represents clients in the areas of taxation, employee benefits, and general business transactions.

She helps small and larger, large employers design and administer executive compensation, retirement and welfare benefit plans, and assists employers with main compliance requirements, including those under the Internal Revenue Code and ERISA. Cindy has assisted clients with IRS plan audits and DOL plan investigations and helps clients identify and correct retirement plan failures.

Cindy regularly advises clients on structuring and operating qualified retirement plans. So thank you and welcome, Cindy. Next, Dan DiGiacomo. Dan is an institutional advisor here at CAPTRUST. And he specializes in helping client or plan sponsors across the defined benefit, defined contribution and non qualified deferred compensation space to navigate their plan level responsibilities and optimize outcomes for participants.

He joined CAPTRUST in 2010 and he has 25 years of experience in investment consulting and financial services. Dan's work has earned him industry recognition and awards from Barron's, Financial Times, and the National Association of Man Advisors. And last but not least, by any means, is John Atchison. John joined CAPTRUST in 2020, and he currently serves as a Senior Team Lead for Governance, Risk, and Compliance of IT Information Security and Network.

John's responsibility is to identify and assess IT risk from multiple sources. He has been in the industry since 2012, and prior to working at CAPTRUST, He worked as an information security coordinator. He holds professional certifications in information system security, governance of I, enterprise IT and risk.

And informational controls. So thank you again, John. so for, before we begin, I just have a little bit of housekeeping. so with our previous webinars, we will not be answering questions during the live presentation today. But we do encourage you to use that Q& A box. to put in any questions that you do have, and that we will get back to you and answer them after the webinar as soon as possible.

So thank you very much. and let's go ahead and get started. So Jon, I'm going to start with you. so can you start with some cyber security basics and you know what we're seeing right now?

Jon Atchison: Yeah, absolutely. Thanks everyone for being online. next slide please. So the topic here is to, you know, avoid scams, but before you can really be equipped to do so, you have to have a good foundation of security posture within your organization.

Cybersecurity basics here essentially cover aspects of protecting the confidentiality, integrity, and availability of information. Otherwise referred to as the CIA triad. Has nothing to do with the CIA government agency. There's a CIA triad. first and foremost, when you think about access control, it's like, who do you, who do you let inside your house, where you live?

Do you let neighbors just walk in? Do you let strangers? Of course not. You have locks on doors. You manage your keys accordingly. Well, it's really no different in the information security world. Strong access control requirements, is really the first step to block and thwart attempts at unauthorized access into a network.

multi factor authentication. has been consistently proven to be about 99. 9 percent effective in stopping unauthorized attempts, even if the password has been stolen on a particular account. MFA is not 100 percent accurate or effective, but it is a very, very strong deterrent and must be in place and enforced in your area of a network.

Additionally, if you can implement a single sign on capability with your service providers, that's another great way to really ensure. safe and stable connections with your resources that you work with on a daily basis. Another great way to just have a strong basic foundation of communication is ensuring that you can communicate in an encrypted fashion over transport layer security 1.

2 or greater over your email system. One area that you can focus on is ensuring or working with your managed service provider. on using what's called a secure message portal. Sometimes you could key in subject line, secure or encrypt or some other keyword. The system will know to route that through a portal.

The recipient of the information will receive a notice that, Hey, you have a secure message from and whoever you are, they click on it, they log in and they can see it, see it in plain text. The good thing about this is it's gated access and it's not You know, free and open to anyone. So look into finding a way to implement a secure communications through a secure message portal.

another foundational aspect of information security is securing your network resources. I'm sure many of you have already heard about the principle of least privilege, maybe to, ad nauseum, but PLP is a very important aspect of any organization's, dividing up of responsibilities across its employees.

For instance, somebody in your legal department does not need access to information security or infrastructure that would allow them to make changes. That division of responsibility is very important. Essentially, the principle of least privilege states that only give the person the access to the resources they need to do their job.

This is very much supported by role based access control. Again, going back to the earlier analogy, If you're in legal, you don't need access to the same thing that finance would, and so forth and so on. Role based access control is a very effective way to have good fences, and good fences make good neighbors.

Another important aspect of making sure that your people have proper access is going to be regular access reviews. What are those? There are a number of tools out there that will allow you to run a campaign where Let's say if you manage five people, the platform would allow you to see the access that your five direct reports would have to network resources.

over time, employees can advance and move on, or even no longer need, a particular resource or a directory. So access reviews help the manager to make sure that on a regular basis, everybody has, everything they need and they're not over provisioned. Sometimes over provisioning can happen over time, and access reviews are a great way to ensure that everybody has everything they need and not anything else.

Another aspect of protecting the confidentiality, integrity, and availability is secured resiliency. a highlight I want to mention here, and this is a strong mitigating tactic against ransomware, is to have encrypted immutable backups, and immutable means you can't change it. It's very important for people to be able to recover.

from such an event. And it is not something that I would want to wish on on anyone in the audience. Having immutable backups that are encrypted will enable you to recover from any sort of data loss scenario. And that's just one aspect of secure resiliency. Another aspect would be having independent third party work with you and assessing your security controls on your network.

If you're in the market for and have the resources to engage an auditor for a SOC 2, that's a fantastic way to really communicate assurance to your clients and your customers that your security controls are up to stuff. A penetration test is another opportunity to have, validation of your security controls.

you can engage, a qualified third party to conduct, an external penetration test where they will simulate what an attacker does. Trying to get in from the outside, they can also run what's called an internal assessment to simulate it. If an attacker got into your network, how far could they go?

What directories could they access? What information could they copy? This is also a very good way to ensure that your fences are also very well put up on the inside of your network as opposed to the outside. There are a lot of other opportunities out there for companies and plan sponsors to have their secure, have their security controls tested.

And I certainly encourage you to investigate, the opportunities. And you can certainly consult with your managed service provider for, possible recommendations. one of the best things that, that we have in the industry is guidance from the Department of Labor. Their cybersecurity program, Best

Practices, gives 12 really, really helpful guidelines to, you know, frame your, your organization by, and to consider.

Well, how are we doing on strong access controls? How are we doing on vendor management? those 12 guidelines are a strong, strong foundation for you to benchmark against it and help build, strong basics of access control along with other areas of having a good security posture. So what are some key areas of focus for plan sponsors?

I'm really want to focus here on, you know, raising the bar of understanding on the threat landscape. Thank you. A lot of times non information security or non technical people will, you know, delegate to somebody to just, just go handle it. Go handle it. I don't understand it. You come tell me what needs to be done.

You know, we don't live in an age where that works so much anymore. And I think it's very important that plan sponsors and people in those leadership positions, step into the arena a little bit and just learn a little bit more about the threat landscape. And the good thing here is you're not going to be, you know, Expected to be an expert in this.

This is why you hire people on your staff. This is why you work with security advisors on the outside. But being able to have a basic understanding of the threat landscape from reading articles, that's going to give you a strong basis to ask questions for the purpose of further understanding. How will my organization, be open to exposure if this happens?

I think working with, Your third party security provider, your managed service provider, or even your internal staff. This will go a long way to building that trust that, A, you know, leadership understands what's going on, they're driving the questions, and they're going to help us get better. Now, you really bring strong business acumen to the cyber arena, and whether it's working with a third party, that's assisting you with your platform, or with your network, or working with your internal staff, You know, good communication really matters, and, you know, moving beyond the initial intimidation of acronyms that typical, you know, IT people speak in, like, I do it too, it just kind of happens.

The important thing here is share and teach about the business processes, make sure they understand. If it's a third party MSP, it'll be very important for you to help them understand your business, where your exposure points are, because they're certainly going to be assisting you. and creating a good cyber posture to protect your network.

You know, combining the expertise from these complementary domains is really going to create a better outcome than if somebody just says, y'all take care of it and let me know what the bill is. It's very important to be actively involved. And again, you're not going to be expected to be an expert in this, but it's very important that you have a modicum of understanding which will propel you to getting a better understanding overall.

You know, vendor management and accountability, these are super big things in our space. You know, a couple of areas that I think are really worth focusing on here are make sure that your contacts are built in such a way That you are requiring your third party to adhere to security standards that you would have on your own network.

If it's good enough for your network to protect the data of your clients, then it should be good enough for your third party. Some places might have a data privacy and security agreement, you know, work with your counsel to figure out what that looks like, but holding them to like standards is going to be a really important thing.

Now watch those T's and C's, it really matters at the end of the day. more importantly, going back to just not saying, Hey, you know, you handle it. You can't ever transfer accountability of, of taking care of your client data. You can transfer responsibility for a function, but at the end of the day, if something happens to that third party, accountability comes back to you.

Again, you know, DLL guidance on cybersecurity. This has been very helpful for, you know, so, so many companies out there. And how does your cyber program compare? to the framework put forth by the DOL. You know, step through it with your technology and security teams. Number one, work through it. 1, 2, 3, 4, 5, all the way through 12.

How do you stack up? Where do you find gaps in what you're doing? Now, remember, these are guidelines. These are not prescriptive, but they provide a great starting point, even in talking with your managed service providers. So definitely leverage that guidance. Finally, you know, cyber insurance is something that Companies have benefited from if they've had a particular event, but it's also a necessary cost or expense that companies embrace on an annual basis.

You know, research the coverage options and consult with your insurance professionals who understand your business. That's a really important thing. If they understand your business, they can help you to really effectively tailor or bring policy options to you that will provide you with the best protection in the event that the unthinkable happens.

So when proper protections are placed, like this is when you start to see headlines in the news and nobody likes the thought of having headlines about their company, especially in a negative light. Assumptions can be costly when it comes to Ensuring that you have a good foundation in your network and even in educating your employees.

Don't assume that your employees know not to click on certain things. Make sure that you're operating a phishing campaign or program that regularly, you know, tests them. And if they happen to click or do something that, you know, causes them to be flagged, make sure that they have training. Don't assume that your security controls are good.

I think that goes back again to having an independent third party assess and test those particular controls. Because if you think something, if you think your door is locked and you come back and it's open. Well, that's an assumption that can be costly. Non validating security controls can and will be exploited.

You know, a lot of times companies may not be a target of intention, but sometimes there'll be a target of opportunity because botnets or other, you know, miscreants out there are looking for companies who have open ports on their network, who have weak security controls that they're looking to exploit and get in.

Internally, unpatched systems are a prime target for opportunistic attackers as well. It's very important to make sure that your operating systems are kept patched and up to date. Definitely work with your MSP and your technology team to ensure that you have a good patching standard in place. Like, how quickly do you patch for a zero day that's been identified?

How quickly for a vulnerability that's considered high, medium, or low? Like, what are those thresholds? just discuss that internally, find out what that risk appetite is, and you know, definitely put something in a policy because this is very, very important. You do not want to be a victim on something that's low hanging fruit, like not having a properly patched system.

You know, unfortunately, negative headlines do await when proper protections are not in place, and it's almost astonishing when you see the things out there where somebody did not have multi factor authentication set up on their account. That's one of the easiest things you can do. I liken that to buckling up when you get into a car.

The seat belt is not going to prevent you from getting into a wreck, but it can prevent you from severe injury or death. This seatbelt or this technology of multi factor authentication really, needs to be in place and, you know, don't, don't be that company. that gets, you know, compromised or put into a bad position because something small like this was not taken care of.

Finally here, I really want to, you know, take to heart, you know, what we're about to say. You know, attackers just don't care about you. They don't care about your families, your career. They don't care if you lose your job. They don't care if your company, is subjected to fines or consequences resulted from their successful attack.

You know, if we're speaking to, you know, right and wrong, you know, moral and more like this is a terrible thing that they just do not care how their efforts will impact you negatively. I mean, good people have lost their jobs over a successful cyber attack. You know, if this doesn't motivate you to really step up and figure out, like, where are we weak?

How can we be stronger? I'm not sure what will. And this is super important. These people do not care about you, and they don't care about your company, your 401k, or anything along those lines. so think about this. Even though it's a faceless enemy out there that we can't see them knocking, they're out there, and they're waiting to get in.

Next slide, please.

So, taking action. And we talked about it in the previous two slides. Start with DML guidance. Start walking through those 12 guidelines. Build a consistent and thorough third party risk management program that focuses on looking at You know, independently validated, security controls via SOC 2 of your record keepers and your key suppliers.

Understand what those opinions mean, qualified, non qualified, adverse, and disclaimer of opinion. Penetration test results. A SOC 2 can be one side of that coin, and asking for, an executive summary of your service provider's penetration test can give you insights into how they did under, a simulated attack.

I think those can really provide a lot of meaningful value. and assessing your own risk posture. Strong contractual agreements. Holding that third party to acceptable security standards is a really good way to have teeth to those great engagements. That's going to make you better and it's going to make them better.

Another important aspect here is to do reassessment on your key suppliers on a periodic basis or a basis that makes sense for you and your firm. Make sure to don't just set it and forget it. Go back, realign, refocus, ask questions. If headlines come out, Reach out to that third party and say, Hey, you know, have you considered this as a possible risk for your firm?

Always, always be quick to engage and don't delay in reaching out with any questions. If you have a good relationship with a record keeper or a service provider, then those phone lines should be open. I definitely encourage you to take advantage of that. Finally, you know, communicate to your employees about scams that could cost them money.

And, you know, one of the things that I'm sure you've heard about would be romance scams. Romance scams is when, you know, somebody lonely gets on a dating app, makes plans to, you know, meet somebody special. Somebody chimes in and says, hey, you're pretty interesting and smart. You spark up a conversation or a chat conversation and that love interest starts to kind of bloom, right?

Then the romance scam takes it to the next level where the attacker says, well, let's meet. I want to meet you. And then oftentimes, I would say almost always, something always comes up where that meeting never happened. And then typically an emergency request will come in for money. And if the scammer has done an effective job of exploiting somebody's loneliness, then the individual, their target is going to be more likely to give money to them.

And whether it's for solving a medical problem or a medical bill or a business crisis or something to say, hey, I need money for this, please. And, and, you know, bear in mind as part of the con here, you know, promises to pay it back are effusive and, and that sort of reassures, okay, no problem. You know, I love you, but paybacks never happen.

And, you know, if the con artist is really into their craft. They're going to try to string this out for as long as they can, and they'll ask for more money, or if the victim license up, that's when the con is over. Romance scams are a terrible thing. You go Google romance scams 2023 2024, and the stories are heartbreaking.

I read one just today where this woman lost nearly a million dollars of her life savings due to a romance scam, and you think about that. Somebody worked for maybe six months or And they got a nearly a million dollar payout. Like, that's just wrong. And these are the kind of things that can happen to individuals, later in life or even early in life where they're a little lonely.

So being aware of these tactics is pretty important. Pig butchering is another term here that's not very pleasant, but the idea here is that the, the farmer fattens up the pig before butchering. Reports typically will indicate the pig butchering attacks have originated in China, and it is very similar to a romance scam where the con artist builds up that trust and then finds a way to bring in a can't miss investment opportunity.

A lot of times this is connected to crypto investing. Typically when that money is gone, the scammer walks away and does not contact anymore to their victim. Sometimes the con artists may try to strain out a little bit more, but pig butchering is a long term con. It's a long term gain where, you know, trust can be built out from six months to even over a year, depending on the potential payout.

So think about this. This is a real deal and just because it hasn't happened to us, I'd be willing to bet that you probably know people in your circle, who are aware of this might have happened to you. finally, and this is kind of scary as being a father, extortion on false pretenses. you go do, another, you know, search and you'll find that attackers can take a snippet of, a voicemail of, of your voice or find a, posting on social media where somebody is talking.

An attacker has a tool that can take anywhere from, you know, a minute to three minutes clip of your voice, and it could create a successful AI persona that could call and impersonate you. I was reading an article today that talked about a woman who got a call from her daughter that was being held captive.

And the, you know, the daughter said that these bad men had me, and thus ensued a lot of terrible things said over the phone. The mother is just panicked. Cannot believe what's going on. It eventually turned out that it was a scam. It was a complete scam and she was ready to make that move. So be aware that with all the promises and, you know, ideal, benefits of using artificial intelligence, you know, the people out there with bad intentions for you and for your money, they're leveraging this.

So be, be very aware that All's fair in love and war. And they're certainly, you know, making a best effort to try to separate people from their money.

Lisa Keith: Thank you so much, John. Yeah, it's just lots of great information there. A lot of really scary things out there. So thank you very much. So Cindy, you know, can you tell us how this is an important from a plant fiduciary basic?

That would be great. Thank you.

Cynthia Boyle Lande: Absolutely, Lisa. If you go ahead and go a couple slides ahead for me. I'll go ahead and get started. All right. So I want to start by laying the stage with Why cybersecurity matters, particularly for ERISA plans beyond the broad issues that you've likely heard about in the news headlines.

The first reason is the risk profile associated with ERISA. As Lisa mentioned at the very beginning of the program today, there are substantial assets sitting in these plans nationwide. The DOL compiles data on an annual basis that they pull from 5500s and other publicly available information sources.

And for 2023, they reported that 153 million employees have retirement accounts, ERISA retirement accounts. Holding over 12 trillion in assets. So there are substantial assets sitting out here incentivizing fraudsters to try to find a way to gain access. The other unique aspect of ERISA plans is that they're largely held by, normal people.

These are not institutional investors. These are not necessarily highly sophisticated investors. These are normal people saving for retirement. And as a result, it's often easier to access these accounts or trick individuals into providing access than it would be with larger institutional and sophisticated investors.

The other reason this matters right now is because retirement plans are becoming a greater focus for the fraudsters. We know they've figured out credit card scams, they've figured out bank account scams, and the retirement accounts within the last five years have really become an increased focus.

Another reason this is significant is the integration of plan operations and technology. You notice as plan sponsors that employers are moving more online with their retirement plans. That's largely driven by employee and retiree demand. They want to be able to access their retirement information and retirement assets in real time.

And there's a balance between that immediate access to retirement accounts and retirement plans. Assets and the elevated security that's needed in this area. And lastly, this is really significant for ERISA plans because of the regulatory expectations around these plans. Plan sponsors and plan committees, retirement plan committees, the different structures that employers have.

These are all fiduciaries and that fiduciary status requires something more than just general commercial. It implies a duty to protect participants and protect their assets in a prudent and careful manner. Next slide. To dig into those fiduciary duties just a little bit more, Arisa turned 52. Just a couple months ago, earlier this year in September on Labor Day.

So ERISA has been in place imposing these fiduciary duties for quite some time now. 50 years ago, I'm sure Congress had no idea what online retirement investing would look like or online retirement plan administration and record keeping would look like. But the rules under are, flexible and they change with the times and, and the most important of those rules is the duty to act prudently.

That implies a duty of acting with care and with skill and protecting plan assets. And there's a little bit of a question in the courts right now on whether that digital data, the participant data counts is a plan asset and courts are moving in the direction of finding that it does at the very least.

Ensuring that there is no access to actual financial or investment assets is something that is required by ERISA. The other places where the courts have weighed in previously are on the selection and monitoring of service providers. There has always been a duty to be careful and thoughtful in selecting service providers, and because a big part of those services being provided now are online access services, Cyber security, those sorts of things that, that should be considered part of that service provider selection and monitoring.

And the other place the courts have weighed in previously is on the continuing evaluation and effectiveness of those service providers. And again, that now includes the cyber security aspects of what they are providing. One thing I always like to highlight when we're talking about ERISA fiduciary duties is that the process is more important than the outcome.

so certainly we want all positive outcomes. We do not want any retiree assets breached. We do not want participant or retiree data to be leaked. But, but sometimes things happen and sometimes participants provide access to, to their own accounts and we can only provide so much information and education to them.

So the key here is to focus on the process and make sure it is thoughtful and reasonable and designed to protect plan assets more so than the outcome. Next slide, please. So John touched on this a few different times, the DOL's cyber security guidance. and what does that look like? The DOL came out a few years ago and issued their first set of formal guidance on cyber security for ERISA fiduciaries.

And just this year they updated that guidance, but it is, it's largely, the same as it was when it was initially issued. The one thing to really take away from this DOL guidance is that it is not a prescriptive list of of steps that all plan sponsors absolutely must take. Instead, the DOL acknowledges that there is no one size fits all.

cybersecurity and the guidance that they have issued instead of being that one size fits all solution is a list of processes and best practices that they encourage plan sponsors to, to consider. and pursue if they determine that those steps are best for them and their and for their participants. So to walk through a few of these areas where the DOL focuses, the very first one is developing a comprehensive cyber security program.

This is one area where we we really do encourage our clients to To start, we have started to see the DOL when it comes to plan investigations, to include questions about cybersecurity and, review of service providers for their cybersecurity practices. As one of the first questions we get when we see an investigation, it it, it's just popping up as a standard question.

The good news for now is that it seems that the DOL is looking for. Some process, some thoughtfulness, even just fiduciaries that can answer the question about what they're doing for cybersecurity. The DOL does not necessarily, or we have not seen the DOL really come down hard on planned fiduciaries who have a practice questioning whether there are some areas where the process could be improved.

So step one is develop that program and if, and if you don't know where to start. Our recommendation is just to start somewhere. Start asking questions, start reviewing agreements, start talking with your service providers so you can figure out what's happening currently and begin to develop that program.

The next piece, once you have that program in place, is to conduct assessments regularly. We know in the investment context and in other areas where the courts and the DOL have looked historically, they don't want to see a one time review. Everyone assumed that things are fine and then no additional follow up or assessment.

That's, that's going to be the case even more so in the cyber security context because this area is changing so rapidly. So continue to complete those risk assessments regularly. The next one, engage with service providers that have strong cyber security policies. You can't know whether your, whether your service providers have these strong policies unless you ask the questions.

So ask the questions, compare to alternatives, get support with benchmarking, just like you would with any other service provider. Carefully review your service provider documents. You want to make sure that your service providers are taking an appropriate level of responsibility for cyber security issues that are within their control.

You want to limit access to the extent needed to reasonably complete plan functions. John spent a lot of time talking about that limiting access to what someone needs for their job, so I won't belabor that. And the last one, providing recurring current participant training. you heard from John that the participants can really be the weakest link.

and this is not an area where we can say it's up to the participants. We've checked with our service providers. We've made sure that our technology is secure. The participants are on their own. I'm going to talk about a few different cases, coming up and in the participant training and making sure the participants are protected is a direction the courts seemed like they're going to be going.

So making sure your participants are trained, making sure they know what it means to set up those good strong credentials, those are all best practices. When it comes to technical best practices, you want to implement access control and identity management, like strong passwords, two factor authorization.

You want to ensure that your outside service providers are encrypting data and providing secure systems, and you want to regularly monitor and update security measures. So something that was perfectly adequate five years ago may not be adequate today, and it's important to continue checking those things.

Lastly, security tips for participants. I want to emphasize again those login credentials. We have seen that it is very common, or maybe more common, for fraudsters to be able to access accounts when participants do not have login credentials set up. They can use other information about the individual, Social Security number, date of birth, all of that data that often can be found online, unfortunately, for individuals now to create those credentials if they don't already exist.

So if there is one thing you push your participants to do, it's to set up those online credentials. You want those to be with strong passwords, multi factor authentication, and then again, being cautious of phishing and suspicious email like John mentioned. Next slide please. All right, so we've talked about what to do to prevent issues.

It's also really important to have a strong incident response plan so that you know what to do if something does go wrong. And there's, there's really four different phases to this. The first is the preparation. So figuring out who's going to be responsible for managing an incident, training that person, making sure that they have processes and protocols that they know how to follow and that they have tools available and resources available if something does happen.

The next piece is detection and analysis, making sure that when something happens, you're finding it quickly and that you can determine what went wrong, so that you have something monitoring your systems and can really dig in and classify the type and severity of the issue once it is identified. The next piece is containment.

and recovery. So trying to stop the problem once you've spotted it and classified it. it's really important to notify law enforcement and insurers, limit the spread, remove the root cause and restore the systems. And then the last piece is what often gets missed. These situations can be very stressful when they're resolved.

Everyone wants to move on and get back to their day jobs, but it is really important to take a look at what happened, debrief the incident, identify whether there are areas that can be improved, and document as well.

So I'm going to take some time to talk about three different cyber security cases that we have seen, and I really like to walk through these because they show how a cyber incident could turn into a legal issue for, for plan sponsors in particular, but as you'll see, these become issues for record keepers, for consumers.

And sometimes for individuals, whether it's the retirement or fiduciary committee or an internal administrator, but that individual who has that fiduciary role with the employer. So I'm going to take these in reverse order. And at the very end, I'll explain why. But the first one I want to talk about is Colgate Palmolive.

And the fact patterns are going to start to sound pretty similar. In this case, the fraudster attempted to change some information online, made multiple phone calls into a data center, and eventually by calling into the data center, they were able to make changes to the participant's email address. Phone number and mailing address.

and, and really interesting in this case is that the mailing address was in a different country. That, that's something that was flagged as a red flag by this participant. They were also able to request new credentials, had indicated they were not able to log into their account, and they had those new credentials mailed to that fraudulent mailing address.

The last things that they were able to do were change bank account information. And request a lump sum distribution. And it took several calls for them to get all of this done. there were processes in place that the record keeper indicated they could not make all of these changes at once because that's, that's a little bit suspicious.

But at the end of the day, they were able to get 750, 000 transferred out of a participant's account. the impacted participant sued the plan sponsor, they sued the record keeper, and they sued the custodial bank. And they alleged that the fiduciaries, which would include the employer and the individuals on their fiduciary committee, had missed the red flags in this case.

The custodial bank who processed that check was let out of this case pretty quickly. Pretty early on, the court concluded they weren't acting as a fiduciary, they were just processing a check. But ke for a pretty long time un settled the case in septe like most settlements, the not disclosed. So we don cost was to them.

but Can lead to a breach of fiduciary duties that can result in a cost to the plan sponsor, and ultimately to, to those fiduciaries as well. And we know in this case that the plan sponsor or the record keeper, the fiduciaries would not have settled if they did not fear for some real. Significant legal risk.

So, something to kind of kind of watch for. And our takeaway on this case is talk to your record keepers. Make sure you know what they would do in this circumstance. Would they be reaching out to someone at your company? Would they be reaching out to the participant? What would their process be? And make sure that it is reasonable.

Next slide, please. All right, here's another, another fraudster case. This time it involved employer Abbott Laboratories. This one also required a number of calls. The fraudster was not able to get this done in a single call, but eventually they did get a, a one time code to be delivered. They indicated that they had forgotten and A password.

So the one time code was delivered to an email address. The facts of this case are not terribly clear, but it looks like the fraudster probably had access to the participant's personal email, and that was how they were able to get that one time code. They were able to request a distribution. However, The the notice of the distribution went out by by regular mail while the part while the fraudsters ability to get into the account to reset the password to get that one time access code that happened electronically and via email and that was one of the things that the participant pointed to here is that if if the record keeper had moved with the same email Speed on notifying the participant that they had moved with to make the distribution, the participant couldn't, could have stepped in and done something to stop this.

So that's, that's one of the issues that they really highlighted in this case. Again, in this case, both the employer and the record keeper were sued for the breach of fiduciary duty. and ultimately in this case, the court found for the planned fiduciaries. But it's, it. It could still be very costly to an employer to go down this path, even if they are ultimately successful.

There were a few really good takeaways from this case. The first one is that the court did not find a clear duty to protect participant data. So things like birth date, social security number, this is the area I flagged earlier that's a little bit gray. Whether those count as planned assets at this point, still a little bit open in the courts, but that was positive.

The other thing that the court said is that it was not a breach to hire this record keeper because they made a mistake down the road. So at the time the record keeper had been hired, the decision to do that was reasonable. Even if they make a mistake in the future, that's not automatically a fiduciary duty breach, which is really positive.

Next slide, please. All right, so I mentioned I'm taking these in reverse chronological order. So the Estee Lauder case, this is this is really the first cyber security case that was litigated that I'm that I'm aware of. And in this case, the facts are not terribly well. Refined in the complaint and the petition, and that's likely because plaintiffs early on really weren't sure what to allege in these cases, but we do have have some facts that are that that I do want to point out.

So, and this one again, we had the multiple distribution requests. And in this case, those went to multiple bank accounts. So the fraudster kept changing that bank account, kept making additional distribution requests. the, we found in this case that the, the plan, Record Keeper failed to check with the participant prior to making a distribution once they received that request that went through without additional confirmation.

There was also no notice sent to the participant after the distribution in this case. The participant discovered this after they went to go check their statements and found that the money had been transferred. Out there was also no catching the parti. The suspicious activity is another thing that the participant argued in this case, and that the record keeper in this case did not have any clearly developed procedures for handling these sorts of requests or catching these types of issues.

So, One of the reasons I like to flag this particular case, since it's one of the earliest ones, is a lot of the things the plaintiffs raised in this case are the areas where record keepers are starting to develop better procedures. It's can they build things into their systems that would, would trigger if you have multiple changes at once.

I know in, in, in the Colgate Palmolive case, we, we saw that some of those things were in place. You know, are there notices going out? We saw In the Abbott Laboratories case that notices went out, but they went via mail versus via email. and so if we take these cases in reverse order, it does show how record keepers are starting to build these things into their systems.

but unfortunately the fraudsters are just a little bit quicker than they are on, on finding these new ways to exploit the system. What we always recommend to clients is continuing making these changes, continuing trying to find areas where you can improve. Like I said, the most important thing is the process.

You know, our, our, our We see our clients are never going to be perfect on all of this. There's always going to be an opportunity for fraudsters to take advantage of participants, unfortunately. But the most important thing is to continue moving in that direction of having more, more perfect procedures in place.

I'll go ahead and turn it over to you, Lisa.

Lisa Keith: There we go. So, Dan, could you take, we have a few moments left, so could you share some practical tips, for planning committees and what we can do to help them?

Dan Digiacomo: Yeah, great. Thanks, Lisa and John and Cindy for, your, your portions. Now that we have all this information, as Lisa mentioned, I'm just going to review some of the practical takeaways and then share some things we see most commonly as best practices that retirement plan sponsors focus on.

And Like Cindy just went through, and with most things that committees handle in ERISA overall, most important thing is the process. So, this topic has become just another responsibility that we see, you know, most clients having to add to their fiduciary calendar. So they monitor and document it however they do, just like any other responsibility.

RFPs for record keepers or revenue analysis, share class monitoring, just kind of like any other, process that they would have on a, on an annual basis to document the difference being, is this is newer, and if you can believe it even more unfamiliar than, you know, investment attribution, float revenue, and other kind of, you know, Retirement industry related topics.

And so as Cindy said, I think having a program is certainly like the most important starting point. and then updating that program, engaging with your service providers. So, so we see those things regularly reviewing documents, limiting access, like John spoke about. I think it's important to note that the DOL doesn't expect committees to be experts themselves.

So as I'm presenting and working with clients on those calendars, You know, even though we're not expected to be experts as a whole, as John outlined, I mean, clearly, expertise is needed to truly understand and evaluate the proper security. So, a starting point that we go through and usually implement with clients is a due diligence report that we actually produce at CAPTRUST.

John's team. along with some of, our other partners internally, one being the, internal group that manages oversight for recordkeeping analysis and due diligence, together, they put together this great report, it's, you know, 19 or 20 pages, and we don't walk through each page with clients, but it's, it's a great starting point, as Cindy mentioned, to document, a process, and it, and it kind of starts by going through just executive summary in the, in the first few pages of, IT security, what types of audits they have, what dates are the audits from, are there opinions, things like that, responses to those opinions, and then super important, the participant protections, those are outlined as well.

So John's team and the others go to get each vendor that we work with, the record keepers, and ensure that we're getting their responses and understanding their participant protections, and then The DOL best practices, as we've talked about, there's 12 questions and the DOL isn't looking for, again, expertise or deep knowledge of each, but it's guidance.

It's a guideline for. what they've outlined, which I think people listen to when the DOL says something, for how, plan sponsors should monitor that. So we go through all 12 questions and send them to our record keepers and, and document how they respond. And then like Cindy said, also track that over time.

And I think it's a really good starting point as a baseline for, first of all, documenting the process with the committee. Thank you, Cindy. Second of all, what ends up happening is a further discussion, maybe a presentation to the group from, the vendors, you know, IT or security groups, but a lot of times a client will kind of take offline the conversation from what the committee does to go over and above and really get into the details of having, you know, okay, our experts talk to your experts at the record keeper and ensure that we're doing everything we can.

And then the participant element is also, you know, really important. So doing everything you can at the corporate level, starting with documenting the process, ingraining it in your fiduciary calendar, making sure that your organization, your, your record keepers organization are talking to each other for any updates regularly that need to be done from security, and then understanding how you're going to work with your different partners to educate, update.

And impact your participants so that, you know, they can understand where the vulnerabilities are, because that's a very sensitive point of entry. And certainly, I think the most common one, so. Kind of short, but sweet for the closing part today, Lisa, from me. But those are just some common best practices that we see a lot of committees and plan sponsors doing.

Lisa Keith: Yeah, thanks, Dan. And thank you to all the participants on the panel today. I think there was a lot of really great information. I know I personally learned a lot here. So again, thank you to the panel. Thank you all for attending. as a reminder, we will be answering those questions that we've received afterwards, but if you do ever have any other questions, please reach out to us or your advisor here at CAPTRUST.

Thank you, and we'll see you in the next one.

Disclosure: CapFinancial Partners, LLC (doing business as “CAPTRUST” or “CAPTRUST Financial Advisors”) is an Investment Adviser registered under the Investment Advisers Act of 1940. However, CAPTRUST video presentations are designed to be educational and do not include individual investment advice. Opinions expressed in this video are subject to change without notice. Statistics and data havecome from sources believed to be reliable but are not guaranteed to be accurate or complete. This is not a solicitation to invest in any legal, medical, tax or accounting advice. If you require such advice, you should contact the appropriate legal, accounting, or tax advisor. All publication rights reserved. None of the material in this publication may be reproduced in any form without the express written permission of CAPTRUST: 919.870.6822 © 2024 CAPTRUST Financial Advisors