Proskauer

[Podcast]: Cyber-theft of 401(k) Accounts

Employee Benefits & Executive Compensation Blog on **January 21, 2021**

In this episode of the Proskauer Benefits Brief, partner Robert Projansky and special guest Garrett Fenton, senior attorney at Microsoft Corporation, discuss cyber theft of 401(k) plan accounts. Tune in as we discuss why 401(k) plans are vulnerable to cyber security breaches, what kinds of cyber security frauds we are seeing in 401(k) plans, evolving litigation on these issues and steps plan sponsors can take to mitigate risk.

Robert Projansky: Hello and welcome to the Proskauer Benefits Brief: Legal Insights on Employees Benefits and Executive Compensations. I am Robert Projansky and on today's episode I am joined by Garrett Fenton of Microsoft Corporation. Today we are going to talk about Cyber Security and Employee Benefit Plans. Let me first introduce Garrett. Garrett is a senior attorney at Microsoft Corporation and he deals with all issues related to employee benefits and executive compensation at Microsoft. That includes Health Plans, 401(k) plans, Retirement Plans and Non-Qualified Deferred Compensation Plans. And in dealing with those plans, cyber security has certainly been a focus of Garrett's on an ongoing basis. So thank you so much Garrett for joining us today.

Garrett Fenton: Thank you for having me Rob.

Robert Projansky: Today we're going to talk about just that issue and I guess the first issue is why are we even talking about this? Why are plans so vulnerable to cyber security breaches? I think the answer is that from a cyber-criminals perspective employee data is juicy; it's not just that there's a lot of it — and there is — but it's incredibly sensitive in nature: social security numbers, birth dates, bank accounts, medical information, beneficiary information and the like. Not only that, participants aren't just employees; they're former employees, so that's an extra bonus for the cyber-criminal. In recent years we've heard a lot about data rich healthcare entities being a prime target of hackers resulting in mega breaches of employee data. It seems to me that employee benefit plans are very close cousins in terms of the kind of data that they hold. What's more, benefit plans don't just hold the data. They share it with a number of different kinds of service providers. They give people electronic access to it and that creates multiple points of entry and vulnerabilities. In the world of COVID that can be even worse. It increased vulnerability with the country working at home. It's not just people at Proskauer and Microsoft where people working at home but it's our record keepers and our in-house benefit professionals our ASOs on the healthcare side. With all of that electronic data getting accessed in various ways that didn't before, that creates a lot of risk. So let's turn to you Garrett; maybe you can start by telling us a little bit about what kinds of frauds you're seeing out there in the world from a cyber security perspective in employee benefit plans.

Garrett Fenton: Sure, thank you for having me today Robert. So you raised a lot of good points that are really top of mind for a lot of benefits professionals and certainly people like myself who are advising plans sponsors and in my role Microsoft. As far as what we're seeing today, we're seeing a lot of cases that are starting to crop up. Certainly in recent times some have very similar types of fact patterns the sort of cybercrime type of cases particularly in the 401(k) context where we have as you mentioned all sorts of rich data from participants that is going back and forth from participants to record keepers and not only the data itself but certainly in the 401(k) or 403(b) context potentially you've got actual funds and quite a lot of them sitting around that a crafty identity thief or cyber-criminal potentially can get a hold of. So we've seen certainly in the last year or so some cases starting to crop up particularly looking at in the 401(k) context where I have been really focused on this where you have again sort of similar fact patterns that have been coming up where unknown cyber criminals, identity thefts are able to essentially access participants accounts, obtain all sorts of data and perhaps, most importantly, actually drain the funds from that account usually in multiple transactions the money going overseas and it's probably never going to come back again. It could be accomplished by accessing participants email password, for example, then the person goes on to the 401(k) platform and clicks forgot password using a participant email and is able to go in and essentially pretend to be that participant and reset the password and do whatever they want with that participants account. Or it could be that the participant in one of the cases actually made a legitimate 401(k) withdrawal and a cyber-criminal was able essentially stop that and hack into the expense account that way and as you said, Robert, more people working from home now possibly using less secure home networks maybe more likely to use a Starbucks Wi-Fi to check their 401(k) or usually just checking their email it really does seem to make this a much more serious risk perhaps than non-COVID pandemic times for sure.

Robert Projansky: I guess the next question really is so if there's one thing I've learned that at Proskauer here for a number of years it's that when there are losses in benefit plans you can pretty much bet that somebody's going to sue somebody. You mentioned fact patterns — are people getting sued in these cases and if so who is it that's getting sued? Is it the record keeper? Is it the plan? Is it everybody? What's happening?

Garrett Fenton: I generally expect that when these types of fact occur that you know there is going to be a lawsuit filed and it's probably going to be everyone that's going to be sued. That's my assumption. I expect the plaintiff to sue you know participants in this case would sue the record-keeper, the plan, the employer, really everybody and we have seen that few cases at least so far. The record keeper, the plan fiduciaries the employer all getting sued. In some cases the record keeper and the employer are then pointing the fingers at each other and counterclaiming against each other for contribution indemnity and in many of the cases the defendants, the employers, the record keeper, the plans etc. will then be pointing the finger back at the participant and saying it really is the participant that's to blame at least partially because again the most likely risk that are going to lead to these types of fraudulent behavior and draining of someone's 401(k) account are going to be participant driven it's things like weak passwords, phishing scams, you know views on secure personal networks so that Starbucks network that's usually what's at least partially going to be to blame for this and I guess the short answer being that I generally expect that everybody will get sued and everybody will be pointing the finger at each other.

Robert Projansky: And so what kinds of claims are being made against the record keeper or the plan administrator in these sorts of cases.

Garrett Fenton: So we're seeing breach of fiduciary duty, claims under ERISA essentially arguing that the employer, the record keeper, the plan, the fiduciaries all had a fiduciary duty to essentially act prudently, which certainly they did to the extent they are fiduciaries. And plaintiffs alleging that they effectively breached that duty by failing to implement you know sufficient controls to prevent these types of cyber criminals to be able to go in and access their 401(k) accounts. Whether it's the record keeper didn't have two–factor authentication a multi-factor authentication or voiceprint type technology that they you know arguably should have had in place to allow the participants to take steps to protect themselves or failing to notice any sort of abnormal withdrawal requests that may be coming in on a participant's account and verifying with a participant that they did indeed make those withdrawal requests. There was one case in particular Leventhal case that dealt with a similar type of facts that I mentioned before where a participant's 401(k) account had been drained in multiple transactions in a short period of time from a cyber-criminal and there was even an email from someone at the record keeper saying something to the effect of you know here's another one this guy is about to be out of money soon but the company never actually alerted the employer or the participant of those concerns and the fact that there was this sort of abnormal withdrawal behavior going on. Allegedly failing to notice these types of abnormal behaviors, failing to react quickly enough, notify the participants, take steps to mitigate harm and remediate you know anything as soon as possible that we're seeing a lot of these cases deriving from.

Robert Projansky: And have Court's ruled on any of these in a way that's sort of helpful for us to understand where they're going with this?

Garrett Fenton: There haven't been any decisions yet on the merits, at least not that I'm aware of, certainly been watching this very closely. There was one case, Estee Lauder case that settled earlier this year so you know with the settlement unfortunately we didn't get any you know helpful case law to come out of that. There's the Leventhal case I mentioned earlier that actually survived the Motion to Dismiss last year. Unfortunately for the defendants there it was able to move forward but has not you know reached the merits yet at least that phase of the case. And then just recently in that same case the record keepers counterclaims against the plan sponsor for contribution indemnity survived the plan sponsor's Motion to Dismiss just recently. So again everyone pointing the finger at everybody. So I guess we can say there's been some litigation developments in the sense that they survive Motions to Dismiss but nothing on the merits yet. And then the other you know big case we have been following — the Abbott Labs case — that similar facts of the cases we've been talking about, Abbott Labs being the defendant as well as the plan administrator. The judge in that case actually did grant Abbott and the plan administrators Motion to Dismiss a little while back but then the plaintiff filed an amended complaint and that is now actually just a few days ago on November 20th Abbott and the plan administrator filed another Motion to Dismiss so that's pending at this point. So there's still a lot to be determined as far as how these cases develop and the case while we may get out of it that's helpful but we're still someone in a holding pattern and waiting to see what happens at this point

Robert Projansky: So while we're in this purgatory of cyber security, Garrett, what do we do? I'm a plan sponsor, how do I prevent problems at the record keeper level? What do I at the participant level? Are there steps I can take you think to mitigate risk here?

Garrett Fenton: Absolutely and I think at this point every 401(k) Plan and the fiduciary committee should have this on their radar, on their agenda they should implementing some best practice measures and there certainly are some best practice measures that I absolutely recommend. I think plans out there would be well advised to put into place certainly three's no way that you can prevent these problems from happening you know at the record keeper level or at the participant level but as much as you can do to protect yourself the extent possible we certainly should be doing that. One thing that I certainly recommend we implement at Microsoft and I've said to my peers as well is ensuring that we have good language in our summary plan description for 401(k) plan to make sure that it's clear to participants at the participant level that they're using strong passwords that they are keeping them confidential that they are implementing multifactor authentication assuming that that's available from the record keeper, establishing voice print or other types of measures and security technology that's available to them and also considering providing essentially a best practice notice to participants perhaps on an annual basis with the open enrollment materials or at some other time just to remind them they've new employees who have recently set up a 401(k) account or a defined contribution account or just need a refresher every once in a while that they need to be using strong passwords and keeping them in confidential and doing all these things to make sure their accounts are safe and putting a lot of the onus on them to do what they can to protect themselves. And then also certainly just doing your due diligence and monitoring — making sure that this is something that's on your fiduciary committees agenda and it's in your meeting materials and minutes that they're keeping track of this and monitoring the record keepers incorporating it into any review of your service providers or record keepers, in the RFPs that may go out you want to make sure this is certainly incorporated into that as a really important factor. And even just looking at your record keeper contracts and seeing if there's language in there to make sure it's clear what happens if there is an incident you know is the record keeper going to make the participants whole? Will they hold harmless and indemnify the plan? Things like that that are certainly best practice measures to implement if we can?

Robert Projansky: I think that makes a lot of sense. You know we sometimes get lulled into a false sense of security we sign contracts how many years ago with our 401(k) vendor — we don't always revisit them because there isn't a whole lot of reason to but I think it's a fair point that maybe it's time if you have one for a little while things change cyber security concerns change and maybe it's time to look back and see if there's anything needs to be updated. And frankly there's nothing wrong I don't think with updating diligence either on an ongoing basis you may have done a cyber security analysis of your record keeper 5 years ago. I think it's fair to say that cyber security 5 years ago is different than cyber security today best practices may have changed over time so having a periodic diligence process seems to make a lot of sense to me.

Garrett Fenton: Absolutely and I would just add too another sort of line of cases that we're seeing that even though it's not directly on point with some of the cyber security issues that I think relevant looking at cases like there's the Harmon versus Shell Case or the ADP Case now where you have participants that are suing plans and record keepers for allegedly allowing the record keeper to use participants personal information to market financial products from the record keeper independent of the plan and the way that's relevant to this issue is it's the underlying concept of whether or not plan participant data is a plan asset and that's essentially what the plaintiff in these cases are arguing and depending on how those case law develops in this area that could be a whole other wrinkle to this if just planned participant data itself is considered a plan asset just like the money that you have in your 401(k) Plan is a plan asset that I think really increases the scrutiny on everything that we're doing in the cyber security space as well.

Robert Projansky: Very fair point and something we're definitely watching as well. See how those cases play out. Well Garrett thank you so much for spending time with us today really appreciate it and thank you all our listeners for joining us today on The Proskauer Benefits Brief. Stay tuned for more legal insights on the Employee Benefits and Executive Compensation and be sure to follow us on Apple Podcasts, Google Podcast and Spotify. Thank you very much.

View Original

Related Professionals

- **Robert M. Projansky**

Partner