How Cybersecurity Standards and False Claims Act Heighten Litigation Risks

December 11, 2025 – SharkCast
by Kent J. Schmidt and Seth Goertz

The connection between changes on the regulatory horizon and the creation of new theories of liabilities in civil litigation is well known. A new regulation often creates or expands a standard of care or obligation for a company that a plaintiff, including a consumer in a class action, can point to as a predicate for a tort or other legal theory. The nexus between the regulatory landscape goes even further. In this episode Kent Schmidt interviews Dorsey Partner Seth Goertz on the unconventional mix between cybersecurity standards and False Claims Act, which empowers whistleblowers to bring lucrative claims for even small deviations. This creates a template for whistleblowing and cybersecurity standards even in the private sector, creating a litigation risk even where there has been no data breach.

Related People

- Kent J. Schmidt
- Seth Goertz

Transcript

Voiceover [00:00:00]

Welcome to another episode of the SharkCast on litigation risks management, where we explore why businesses are so frequently sued, and how to mitigate and navigate the dangers lurking in these risky waters. Join us now as we welcome our host Kent Schmidt, Litigation Partner at the law firm of Dorsey & Whitney.

Schmidt [00:00:25]

Welcome to another episode of SharkCast. You know, in thinking through, writing, and

speaking about litigation risk, we often refer to the connection that exists between changes on the regulatory horizon and the creation or spawning of new litigation risk. And there's clearly a very significant connection between the regulatory world and litigation risk. For example, a new regulation can create or expand a standard of care. It can be pointed to by a litigant as evidence of a breach, of a duty, a tort, a violation of another statute, and so we want to keep an eye on what's happening in the regulatory world, and even what's happening with criminal prosecutions, because that informs our approach to mitigating litigation risk. And I can think of no one better to invite to the SharkCast virtual studios to address this in general, and more specifically, how cyber threats and cybersecurity standards in a particular area of federal contracting can impact litigation risk, than our relatively new partner, Seth Goertz. Seth joined our office from the U.S. Attorney's Office in Phoenix, and he's been at Dorsey for a relatively short amount of time, so I don't know him that long, but Seth, welcome to SharkCast, and welcome to Dorsey as well.

Goertz [00:02:03]

Yeah, thanks Kent, appreciate it. Glad to be here and enjoying my time at Dorsey so far.

Schmidt [00:02:09]

And how long have you been at Dorsey?

Goertz [00:02:11]

Joined, yeah, in March of 2024. So, I guess it's getting on to be about 18 months now, so year and a half.

Schmidt [00:02:17]

Okay, well, let's, before we get into this, let me ask you a little bit about your prior work at the U.S. Attorney's Office because I think that's going to impact your perspective on the topic we're going to be discussing today. What'd you do in that career before joining Dorsey?

Goertz [00:02:40]

Yeah, sure. So, I was a federal prosecutor in the white-collar section of the U.S. Attorney's Office in Phoenix, and so the work, easiest way to explain is it's split between, for me, traditional investigating, prosecuting, going to trial, and traditional white-collar frauds. Which include, like, healthcare fraud, investment fraud, other types of business-related frauds that rise to the level of the crime, and then, that was about half of my work and the other half I focused on cyber related fraud. And so I worked the FBI in Phoenix as a cyber division and I would work with them, sometimes even in a SCIF, a secure area that you have to have top secret clearance to even be in, and would investigate and prosecute cyber related crimes, and those are very parallel to what we see today a lot in related to like, network intrusions and cybersecurity. Those events will happen. Bad guys

will come in, infiltrate a system, take data, take money, and then businesses will obviously have to do things to mitigate those risks, but when the FBI comes in, they are then looking to try to find the bad guys to figure out what they did, where they're located, and the trickiest part of that is putting someone actually behind the keyboard that was involved in the crime and then charging them. And so it was a fascinating, fascinating experience that I enjoyed a lot and have now parlayed that into a similar practice, just from the other side, where it's defending individuals and entities involved in regulatory inquiries, criminal offense, but I also do a lot of cybersecurity related counseling, guidance, sort of post-incident mitigation, drawing on a lot of what I learned at DOJ about how the cyber threat landscape is currently today.

Schmidt [00:04:27]

Okay, well let's, that's a perfect segway to where we're really gonna get into the meat of our conversation, and that is cybersecurity, the federal standards, prosecutions of companies under the federal standard, specifically federal contractors, as well as a different angle, which is whistleblowing through False Claims Act. It's not something you have traditionally heard of before. So, some things that you've written, Seth, caught my eye and I would like you to sort of unpack what's going on in the last couple years on cybersecurity standards and False Claims Act.

Goertz [00:05:15]

Yeah, yeah. We are, I mean, this is a space that continues to evolve very quickly. I mean, almost daily, hearing new, yeah, new evolutions really. And one of the main shifts, just broadly, sort of on a philosophical level, is that we're starting to see, and we're entering a phase in which cyber incidents, the broad loss and disclosure of personal identifying information, accounts, the stuff that we kind of just now take for granted is occurring. Regulators are starting to see a shift in that they are determining this is no longer okay. Like, we want to do whatever we can now to stop this from happening, and we are going to start enforcing certain regulations and basic protocols that businesses who possess this information need to be complying with, and this is beyond just data breach notification and how to possess, you know, PII, like we have all of the broad data disclosure, data retention obligations, but we're getting into the actual cybersecurity protocols and certain things that need to be done to protect a system. Those are slightly different, and one of the main ones…

Schmidt [00:06:26]

Let me just interject here and make sure that our listeners understand the distinction.

Goertz [00:06:30]

Okay.

Schmidt [00:06:31]

We have an entire world out there relating to data breach and what happens when there's been a data breach. For a private company, disclosures that are required to consumers, to the attorney general, some other regulator. This has nothing to do with that in one sense, I mean, obviously commonality. Is what you're saying is that this relates to the standards even if there's never a data breach?

Goertz [00:06:59]

Exactly, exactly. And you are right. They do relate, 'cause one sort of leads to the other. You don't get the breach often without sort of an infiltration to your network on a basic level, right, and the regime we currently have is sort of post-incident requirements. Post-incident requirements and other basic regimes for what entities are required to do what with certain types of information, right? So, if you're a healthcare entity, you have certain regulations regarding the HIPAA and your various patient information, treatment records, stuff like that that you have to possess, and in the event of an incident, you gotta notify people, like you said. What we are seeing though now, is that regulators are starting to look at, what are the actual technical specifications that these companies are employing to protect this data on the front end, right? What is going on with their actual network security? What type of testing are they doing and how regular is it? How aware are they of, sort of, their vendors, their networks, the data that they're possessing? What are they actually doing from a technical capacity to protect this information? And that actually becomes far more important than I think people realize, because entities that receive federal funds, federal contractors, will receive those funds and their contracts signed various attestations. In one of the attestations they're now signing, is relates to their cybersecurity protocols. This is very important when you get to, like, Department of Defense, and other various sensitive information where there are pretty specific frameworks that companies are attesting to, and even that is beginning to be far more particularized as to the specific type of cybersecurity framework that is being attested to, okay? And so now that actually becomes very important. It's a little different than just these notifications, it's stuff you have to be doing on an ongoing basis and it doesn't matter whether you've had a breach or not and so what we have seen is that formalization with the Department of Justice is called the Civil Cyber Fraud Initiative which is going and assessing whether or not recipients of federal funds are actually complying with the cyber security protocols they've attested to, regardless of a breach. And they're bringing actions, based upon whistleblowers, against entities who have not complied simply with the attestation regardless of the incident. And we're seeing significant settlements already, significant actions in this space, and that is one that I think sort of demonstrates the paradigm shift sort of best in this space.

Schmidt [00:09:33]

Yeah, it sort of reminds of every once and a while I will look outside my office door and I will see the fire marshal walking through doing an inspection making sure that the, you know, hallways, there aren't obstructions, there's fire extinguishers and so forth and what we're seeing is, even if there isn't a fire, the equivalent of the fire marshal in the cybersecurity realm is more and more focused on federal contractors. Now let's talk

about the way in which False Claims Act, which is something we haven't seen in cybersecurity, is being brought to bear in this area and maybe for our listeners that aren't as familiar with False Claims Act claims or theories, or that body of law…

Goertz [00:10:26]

Yeah.

Schmidt [00:10:27]

Can you unpack that a bit for us?

Goertz [00:10:29]

Yeah, so the False Claims Act actually is a very old law, it dates back to the Civil War, and it's basically the government's effort to police recipients of federal funds to make sure they're doing with the funds what they said they were going to do. They're not wasting them, prevent fraud waste and abuse. And so, the False Claims Act is a mechanism for the government to go after contractors who have failed to do what they said they were going to do with the money they received, basically. And the way in which they do that is often through whistleblowers and so the reason this is such a powerful tool is because the penalties under the False Claims Act are extreme. On a basic level, you get triple damages and so the government can triple, they will, this isn't always how it works out, but the government will often start their case with whatever contract you received, triple that and that's our damages. And the whistleblowers get a portion of that, often a third essentially is what they can initially expect or attempt to claim…

Schmidt [00:11:26]

A bounty of sorts.

Goertz [00:11:27]

A bounty, yeah exactly. Exactly. And so, these cases will start often by a whistleblower bringing suit and filing a qui tam action. The government then has a certain amount of time to intervene on this behalf or let the relator, as they're called, go forward with the suit. And so what, you typically see that in industries where federal funds are routinely granted. You see this in Department of Defense related contracts, you see this in healthcare a lot. Healthcare is a common space where this is used and particularly related to Medicare violations and enforcement of different billing fraud. You see it, sort of, Medicare pharmaceutical related stuff but we haven't seen it in cybersecurity space, and this is very novel. Under the Biden administration, the DOJ established what was called the Civil Cyber Fraud Initiative and it is, like I said previously, to use the False Claims Act to ensure that federal contractors are complying with their cybersecurity protocols that they attested to. So using the False Claims Act as a tool to enforce this and, you know, as you can imagine, it's a pretty powerful tool if your, you know, the contracts you are receiving are the basic starting point for damages and they're going to

look at what box you checked in which cyber protocols you said you were going to attest to and it becomes even more interesting and, I think novel, novel's not the right word. The nuance is slightly different in this cyberspace because a typical whistleblower, the whistleblowers in this space, the relators, receive a tremendous amount of scrutiny because a lot of these cases, the relators are just very important, there's no way to get around that. And in the healthcare setting, relators can range from a front desk staff to doctors, potentially, but they sort of span the gamut. What we're seeing right now, though, initially, the Cyber Fraud Initiative, is that some of these whistleblowers are like the Chief Information Security Officer, for instance, so these are whistleblowers that have, you would think, complete insight into the actual cybersecurity framework and protocols, what is happening and, I don't want to say unimpeachable, but that is a very strong, from the government's perspective, if you're getting a relator who is an executive level employee with full oversight on how an entire program is run, that's not often the case with relator I would say, that is a very strong relator, something you are going to take seriously. And you're seeing the result of that, at least for the most part, with some of the early settlements that have already occurred under the Cyber Fraud Initiative.

Schmidt [00:14:04]

They know where the bodies are buried.

Goertz [00:14:06]

Exactly, exactly.

Schmidt [00:14:09]

And has that initiative continued full steam ahead with the transition to the Trump administration?

Goertz [00:14:15]

It seems so, actually. And one of the, there's been a lot that's been said about the DOJ, we don't need to get into, and in every administration, there are prosecution priorities that change, right? And in this one, there's much more of a focus on violent crime, immigration, less so on, sort of, criminal fraud in certain respects. What hasn't though and what we have not seen over the last almost year now, and what people I think were waiting for, is well what's going to happen in this healthcare fraud, the False Claims Act, and the Civil Cyberfraud Initiative. Those have remained relatively intact both in terms of like manpower, like you're not hearing about exodus of prosecutors or AUSAs from those groups. You're seeing continued enforcement, and you're even seeing a signal that we're going to continue to bolster the focus on, like, health care fraud, False Claims Act, and the Civil Cyber Fraud Initiative. So…

Schmidt [00:15:12]

That's interesting. It's interesting it's one of the perhaps few areas in which there's

continuity between the administrations, at least apparently, because it seems virtually everything else that I'm reading about is, you know, completely changing priorities and discontinuing something or starting something new but there's apparently some threads of continuity.

Goertz [00:15:40]

There is and it's interesting. I think people have been cautiously cautious in their assessment of this and not wanting to prognosticate too quickly because of how rapidly things have changed. What I would said is unique about the False Claims Act, though, is that in where it is in some ways different, it derives a tremendous amount of money for the government like these are funds that are recouped, whistleblower payments go out, but the government retains the money, I mean they're recouping money the government paid and huge amounts of monies and so that's where, it would, it would be quite a significant move for the DOJ to really ramp down or not prioritize in a different spot False Claims Act enforcement because of , sort of, just the amount of money that's an issue there.

Schmidt [00:16:26]

Right, right. Well the issue that I think carries over here is the, to even non-government contractors, is the cybersecurity threat, even if you're not a Department of Defense contractor or Medicaid, you know, funds recipient, you have cybersecurity threats and you also have whistleblower protections for employees that are invoked all the time by employees that are looking for a reason to hang onto their job and to, you know, put the, shroud themselves in some sort of heroic whistleblowing context as they're being shown the door. Could this model of marrying the whistleblowing concept with cybersecurity end up being a, essentially the template for more civil litigation that sort of, is patterned after this?

Goertz [00:17:35]

Yeah, and I think that is exactly why this is such an interesting paradigm shift and important to see because I think you could certainly see states, for instance like California which already have very robust regulations for privacy, compliance regarding the possession of personal information. You could see a state like California saying okay, if you're a company subject to these protocols regarding privacy and data, these are also cybersecurity protocols you need to be adopting. And if you are not, here are the potential penalties and I think that is where this is going. I think, one thing to get into sort of civil litigation, is this is a component you are seeing more and, actually, in civil litigation, this space, this sort of class action cases that follow on the data breach cases is that this should never have happened because here are the basic cyber protocols that were not implemented. And there are now, sort of, basic standards that exist for cybersecurity based upon certain industries that are just, you can find online anywhere, right? And this is a good one and, sort of, everyone could be doing that as a baseline. And that's what I think is, when I saw a philosophic shift, that's what I think is the biggest difference is five years ago, it was a cost-benefit analysis for companies in terms of how

much money to put into their cybersecurity infrastructure to prevent a data breach and sort of attempted civil litigation that follows it. It's still a cost-benefit analysis but now there's a lot more of a hammer than just, and not to say class action isn't a big hammer, that's significant, but now you're having regulatory requirements and so it's not just that in the event something happens, it's no, I have to have this as a baseline and if I'm not, at any moment the government can come in and hit me with that and then now there might be follow on class actions, regardless of the breach. And if I do have a breach, now there's all this other baseline standard of care that I would have always required to maintain that I may not be able to show and that's going to make this class action significantly more problematic.

Schmidt [00:19:33]

So, we really follow a pattern in these podcasts where we spend about twenty minutes talking about things that, at least for some listeners in the relevant industry, raised the hair on the back of their necks in terms of how scary things are. We try to turn to some more pragmatic takeaways and steps so let's do that now. Enough of the scary stuff, what are the things that you are working with clients on and the consultants that are being retained and so forth to essentially audit these compliance issues?

Goertz [00:20:14]

Yeah, I think the biggest one is that you want to have and this seems self-serving and it's actually not, you want to have an attorney and a forensic investigator who are doing proactive testing, compliance to ensure your framework is operating the way it should and as the space continues to evolve you are updating and taking account of that and doing quarterly testing, yearly, extensive tabletop testing, is what it's called. And the reason you want to have an attorney engaged or forensic investigator, as they're called, is so that whatever work the forensic investigator is doing and all the profit, they're gonna find some gap. Like there's just no system that's perfect, there's always gonna be a gap. But you want that analysis to be under the cover of the attorney/client privilege so that if you have some issue, that analysis isn't disclosed automatically and anywhere. I can't tell you how many times, even post-incident, where I get a call from a client, we had this issue, don't worry, we got a forensic investigator in and they got their report, and here it is. And I just, my heart it's like every time, and it happens more than you would think. And it's sort of you understand the clients. Like, that was the right instinct, but they don't realize, you've now created significantly more problems because now there's a report out there that is talking about all the things that weren't done because you're always gonna find something, but now it has to be disclosed because…

Schmidt [00:21:33]

It's a very nicely written smoking gun.

Goertz [00:21:36]

Yes, yes, exactly, exactly. And now this person you had, who was doing all this

investigation, is now conflicted off ‘cause they’re gonna be called to testify and you can’t have them continue to do stuff, so you need to bring someone else in. So, it’s just having, I would say the best piece of advice is proactive compliance where you are, sort of have your team in place. And it’s a kind of a multi-facet there. But…

Schmidt [00:21:59]

No, no, please, finish that thought.

Goertz [00:22:03]

multi-facet, where you have cybersecurity, sort of expertise, along with your counsel to ensure that it’s protected by privilege, but you also wanna be interfacing with, like, your data privacy experts who also be sort of staying current on what is easy to retain, how long it needs to retain, what type of information is subject to a retention policy, ‘cause that’s a constantly evolving space, and retaining data is hugely expensive and burdensome, and sometimes you don’t need to retain it for as long as you think you do. And that is only gonna be positive in this space. So, there’s just a little bit of medicine on the front end makes a huge difference to sort of the outcomes if something significant were to happen.

Schmidt [00:22:45]

You know, I think the most common thing I say in this context is the old Ben Franklin ounce of prevention worth a pound of cure, and it applies here as well. I wanna go back to what you had said about doing the internal assessment, the tabletop audit and so forth. If breaches are found, not breaches, if deficiencies are found, is there a duty to disclose, or is there, is it advantageous to disclose to prevent, you know, it’s the age-old question, to prevent or mitigate and/or obtain favor if there’s a later prosecution?

Goertz [00:23:23]

Yeah, yeah. So, I guess there’s two things there. What you want to be, have your forensic investigator find or just the gaps in the network where someone could get in and do something bad, right? What you hope you don’t find is that there is someone in there and there has been a breach. If you do get in and find, and if at some point it’s disclosed, and I have a good example of this, that you’ve had a breach or you’ve lost information, you have to take immediate measures to understand the significance, the scope, and what your reporting obligations are. I mean, absolutely. And I think a good illustration of this was a year or so ago, sort of public lawsuits now related to it is this enormous AT&T data breach that happened I think about a year ago. And that one is very instructive because it was in 2019 that AT&T was sent a ransom that they had a data set that was taken, that was gonna be published to the dark web, multiple data sets. AT&T didn’t do anything. They ignored it, which is, okay, that’s a business decision, that’s fine. But they didn’t even perform an internal investigation to confirm where this occurred. And so, they had no idea whether it had or hadn’t and they didn’t do anything to determine that. Couple years later, similar ransom threat to disclose this, ignored. Again, no internal

investigation to determine that, no advance reporting. And then finally it gets released on the dark web, and now you're sort of seeing the, I mean just an enormous fallout. And what I would say is instances like that happening five or six years into the future, this is just not going to be palatable at all and you're gonna see intense regulatory scrutiny if companies are aware of instances and they don't look into them because now you're starting to get into the realm of significant civil and potentially even criminal liability for stuff like this. And so that's where I would be, you're talking about proactive prevention. You're hoping you don't catch that. That's often not what's caught, is sort of a breach as it's occurring. But you can, and you want, you absolutely wanna act quickly there, but this sort of proactive hope is you just were able to identify the gaps because you have a good forensic investigator who is acting like a bad guy, trying to figure out where can I get in, where are the vendor vulnerabilities, where is this sort of lowest common denominator space for me to access. Like a great story of this is Pentagon did some penetration testing, and they had the weakest link because they had a vending machine that was accessing the network because there was automatic payments, and that sort of compliance protocol for the vending machine payment processing spot, right, was linked to another network that had some spot to get in. And so, you just, people don't realize that, you know, we are very connected and there's a lot of benefit to that, but as a result of that, like, our networks are far more sprawling that you even sometimes realize.

Schmidt [00:26:09]

Yeah. So, to recap, if there's a breach, the disclosure obligation is pretty clear. But if it's just…

Goertz [00:26:16]

Yes, depending on your state. But for the most part, yes.

Schmidt [00:26:19]

Right. But if it's not a breach, and we're not really getting into state-by-state data breach disclosure obligations, which is a whole 'nother conversation. But if there's not a breach, you're a federal contractor and you just have noticed that there's some gaps in your cybersecurity that need to be tightened, some bells and whistles that need to be adjusted, is there a disclosure obligation on that to go to the government and say hey, we noticed we didn't have this protocol and we now do?

Goertz [00:26:49]

I would think, so it's a case-by-case basis so I'd be a little careful. It would depend on how, what the delta in that gap was.

Schmidt [00:26:55]

Right.

Goertz [00:26:57]

But I would be careful for sure, yes, and I would want to assess that pretty closely, and that's why I would wanna be doing routine, testing routine, sort of auditing essentially my cybersecurity program because that is now the standard if you're a federal contractor is that you are actually implementing what you've attested to, and these attestations as to the frameworks are very, are becoming very, very specific. And so yeah, you want to take that seriously for sure. Because…

Schmidt [00:27:26]

And I don't know, talking to a lawyer, maybe a former U.S. Attorney like you, right, to assess that sliding scale of a voluntary disclosure.

Goertz [00:27:36]

Yes, yes, because you know who's gonna be in the room when you sort of do the testing to determine what your gaps are? Your who will know exactly what the network was, will likely be aware of the contract, who will understand what these sort of whistleblower how lucrative that could be, and so you wanna make sure you've taken that very seriously.

Schmidt [00:27:55]

Right, right. Well, these are some very interesting but also sobering developments in the world of cybersecurity, now infused with False Claims Act additions. And so, I appreciate this conversation and all the practical takeaways that you've given us, and our time is about up for this episode and for that discussion. But before we let you go, we reached now the component of our episode in which we call The Deeper Dive, in which we learn a little bit about our guest and the life that they live and pursue outside of the four walls of the office, and outside the pursuit of serving clients and their communities in the legal arena. So, I don't know you very well, haven't, since you're new to Dorsey, but I understand that one of your pursuits there in Phoenix where the weather is tolerable, is mountain biking. Tell me about how you got into mountain biking, and hopefully it's been a pretty safe pursuit for you, and what some of your goals have been in mountain biking.

Goertz [00:29:18]

Yeah, yeah, well thanks. Phoenix is a fantastic outdoor city for most of the year. We're about to get there, we're hitting October. From October to May, being outside in Phoenix is hard to beat, and one of my favorite sort of outdoor hobbies is mountain biking. We got two young girls, seven and three. So, I don't have as much time for this right now as I would like between chasing them around. I live, you know, minutes away from some just fantastic trails, and I enjoy getting out, decompressing, riding, and it's just incredibly beautiful. I got into it, I was a road cyclist, kind of like yourself, for a while. And you had some buddies and friends who were constantly chirping about how enjoyable mountain biking would be. And I just did not believe them. But during Covid, for whatever reason, I got a wild hair, I was like I'm just gonna, there was a great sale on a mountain bike from

a local shop. I said I'm just gonna try this, and if it doesn't, if I don't enjoy it in a month I'll sell this bike. And three months later I sold my road bike 'cause I just, I enjoyed mountain biking so much. I enjoyed being able to just disconnect, which I feel like I'm able to do a little bit better on a trail than like on the road where I'm worried about cars and just, it just feels different. But my goal ultimately, and who knows if this will ever be achieved, is to do the Leadville 100, which is a 100-mile mountain bike race, race is an odd word for it but sort of suffer fest I guess, in Leadville, Colorado, a town that's at 10,000 feet elevation.

Schmidt [00:30:46]

All finishers are winners.

Goertz [00:30:48]

All finishers, yes, yes, and every finisher is absolutely a winner. And the thing I say, if that wasn't enough in terms of how sort of epic this event is, Lance Armstrong, at his height, did this and set the course record, I think the course record's actually, someone beat that. But a long-standing course record, when he was at his height at like seven hours or something. So, this is.

Schmidt [00:31:11]

With any performance enhancing or not?

Goertz [00:31:14]

There might have been. I mean, there might have been. This was sort of at his height. So, like, it's, he was certainly hard to tell.

Schmidt [00:31:22]

Yeah.

Goertz [00:31:23]

But it's sort of like always been, and I have some friends who've done it actually, and it's something that's on the bucket list for me.

Schmidt [00:31:31]

So, what's a more typical time for that? If Lance Armstrong has seven hours and change, what's…

Goertz [00:31:39]

For someone like me, it would be, you know, nine to ten hours probably on the bike. And you're sort of taking some breaks, but I mean it's a full, full day of riding.

Schmidt [00:31:52]

Yeah, well good luck on that. Hopefully you hydrate. When you're mountain biking in Phoenix, are you able to, if you go in the evening as the sun's setting, are you able to do that year-round, or are there just some months where it's just, even at 8:00 at night it's just a non-starter?

Goertz [00:32:13]

I used to be a little bit tougher, and I would just get up at like 5:00 am and go ride, and you can do that all year if you're willing to get up early. Now the weather, you go out in the middle of the day, it's just beautiful so that's great. I think I don't really have an appetite anymore to just suffer in the heat that early, so I kind of for the last few months in the summer just do the Peloton and I do that and sort of, I've grown soft.

Schmidt [00:32:39]

Yeah. And injuries so far have been not too devastating? Falls here and there?

Goertz [00:32:46]

You know, knock on wood, knock on wood, I've had some falls, you know, but nothing too devastating at all.

Schmidt [00:32:51]

Not into a cactus, I hope.

Goertz [00:32:53]

Yeah, not into a cactus, that's right. So, we'll see. About to enter a new season, so hopefully we'll touch base in May.

Schmidt [00:33:01]

Okay. Well, stay safe out there.

Goertz [00:33:03]

Yeah.

Schmidt [00:33:04]

And thank you so much for taking the time to be on SharkCast and it's been a pleasure to get to know you better through this process and our conversation, and I look forward to further opportunities to connect on these things.

Goertz [00:33:19]

Absolutely, thanks for having me, appreciate it.

Schmidt [00:33:21]

As always, I'm indebted to the extraordinary team at Dorsey for making this podcast and episode possible. For many resources on this and other litigation risk, go to litigationrisks.com where more information can be found, including a book on managing litigation risk written by yours truly. Until next time, my friends, this is yet another reminder that there are a lot of sharks swimming out there in the murky waters, so swim safely.

Voiceover [00:33:49]