Transcripts are generated automatically using AI and may contain errors or omissions.

Rich Meneghello (00:00)
Welcome to The FP 5: Five Things for Your 9-to-5. We help employers make sense of the fast-moving world of workplace law and compliance by breaking topics down into five parts. I'm Rich Meneghello, Chief Content Officer here at Fisher Phillips.

Imagine a college football staffer arrested for emailing his old team's recruiting evaluations to rival schools. Or imagine an engineer for Google convicted of walking off with the company's AI secrets. Or even an NBA basketball team accused of planting a mole inside a rival's video room. Trade secret thefts can happen in any business at any time, and it usually starts with an employee on the way out the door. So what counts as a trade secret? How do you protect yours? What do you do when one goes missing?

There's nobody better to walk us through all those questions than Michael Elkon. Michael is our guest today. He's a partner in our Atlanta office, and he's the co-chair of the firm's Employee Defection and Trade Secrets practice group. He spent more than two decades handling non-competes and employee rating and trade secrets disputes. And he's even appeared before the Georgia Legislature's Judiciary Committee when it was considering the state's non-compete statute. Michael, thank you so much for being on the show.

Michael Elkon (01:16)
My pleasure. Thank you for having me on, Rich.

Rich Meneghello (01:19)
Before we get to the five things, Michael, tell us your origin story. How did you become a trade secrets lawyer?

Michael Elkon (01:24)
I became a trade secrets lawyer purely by chance. I was a summer associate and then a junior associate at another firm, and the two partners who did a lot of non-config trade secret work I just liked and I enjoyed working with them. It was purely a personal matter. And then they essentially sold me on this practice as being one where you go up against other, sort of, top litigators. It's business-to-business litigation that's of extreme importance to our clients. They take it seriously and if you do a good job, you know, you become sort of a hero to them. To dovetail with what we're gonna be talking about today, the college football term for it would be “you have high strength of schedule, in terms of your opponents.”

Rich Meneghello (02:17)
All right, so let's dive into the five things, Michael. The first thing we're gonna talk about today is that your trade secrets are probably broader than you think. I know when you ask a lay person or maybe somebody not as experienced in this area, they might think the Coke formula or something like that, locked in a vault. But we know that, in our practice, trade secrets are broader than that. So what does the law actually protect when it comes to what trade secrets are?

Michael Elkon (02:45)
Sure, and I would say most businesses have at least something that they consider to be a trade secret. The way that I often describe this to clients is “What is the piece of information or category of information that you would be most concerned with if an employee walked out the door and took it to a competitor?” So it can be anything

relating to the business; the most common kind of trade secret is customer information, customer lists, contact information, order preferences, pricing, et cetera. But anything regarding your business, if it is non-public and valuable to you, can be a trade secret as long as you take steps to protect it.

Rich Meneghello (03:26)
Okay. And I hinted at this in my little intro, but you recently wrote an Insight that we'll link to our show notes so people can read more about it, about a college football case from Auburn. Walk us through what happened there. I think this is a good example of demonstrating that trade secrets can be pretty broad, not just a customer list or some secret formula.

Michael Elkon (03:50)
Sure. So what happened was there was a player personnel scouting assistant, which is quite a mouthful, working for Auburn by the name of David. And David was involved in scouting, which meant watching tape of high school players and scouting them for, you know, whether or not they would be appropriate for Auburn to recruit: "Is this somebody who can play at an SEC level?" You know, "Does this person fit within our schemes?" And "Do we want to go after them and how hard do we want to go after them?" And he accumulated all sorts of reports on these players. And then he was fired for I don't know what reason, but then he started reaching out to other schools. And calling himself 'Don Julio.'

Rich Meneghello (04:48)
Yeah. Which is the best part of the story, by the way.

Michael Elkon (04:52)
Yeah, it's one step removed from when Mike Vick called himself 'Ron Mexico' to hide himself when he was doing certain things that might cause public embarrassment.

Michael Elkon (05:02)
So 'Don Julio' was offering Auburn scouting reports to other rival schools. I assume some combination of anger at getting fired and desire to make money or desire to get a new job. I mean, these are all sort of common motivations that can come up in a trade secret scenario.

So anyway, these rival schools, smartly, at least one of them, reached out to Auburn and said, "You may want to be aware that your scouting reports are being offered by 'Don Julio.'" And Auburn got law enforcement involved. They essentially ran a sting or did investigations that law enforcement is very good at doing. And they ended up charging David with a variety of trade secret offenses and computer tampering under Alabama law.

Now it is also important to mention these are based off of news reports. David is gonna have his day in court. There's a presumption of innocence. We're not saying that he did this, that he violated these statutes, simply that these are the allegations and this is the description of the criminal charges that have been brought against him.

Rich Meneghello (06:22)
When you help a client take an inventory of what they need to protect, if somebody calls you and just says, "This is what we are we are protecting, this is what we want to protect," what do you what do they most often overlook?

Michael Elkon (06:33)

These days it's a constant competition between technology and trade secret protection. So like technology keeps advancing to make it easier for people to take things. And just as employers sort of catch up to one way of taking things, employees invent new ways to do it. So for example, I got into this niche 23, 24 years ago, something like that. And I think one of the first cases was a financial services case where a guy was leaving and he and his assistant came in over the weekend and printed out all of his client files and walked out with bankers' boxes. Like in 2002, that was your way of stealing.

Now you could put all of that on a thumb drive in 30 seconds, right? And then people have realized that thumb drives are something that a good forensic expert can figure out that you used it. So, you know, some people are taking screenshots of their computer or they're using AI to sort of exfiltrate things. They're using cloud-based accounts of varying sophistication. So to answer the question, it's sort of a constant iterative process where employers need to think about what technology is available and how do they best make sure that employees aren't taking things using that technology while still giving them the tools they need to do their job on a day-to-day basis.

Rich Meneghello (08:08)
Gotcha. Okay, makes sense.

That brings us to our second thing. It's only a secret if you treat it like a secret. So courts often look at the phrase “reasonable measures,” that employers need to show that they took reasonable measures to keep things secret in order to gain the protection of a trade secret. So what does reasonable actually look like? In practice, when you've seen this playing out hundreds of times, what does reasonable really look like?

Michael Elkon (08:41)
First of all, reasonable doesn't have to mean perfect, right? You don't have to be airtight. So for example, some employers have restrictions on what their employees can do with thumb drives. Like they can't even put a thumb drive into a USB port and utilize it, right? That's obviously a really useful way to prevent the exfiltration of trade secrets, but it's not necessary. You don't have to show that in order to demonstrate reasonable means.

Generally speaking, there are a variety of different categories and you wanna be able to put them all into a complaint if you ever bring a trade secret case. So you're gonna wanna be able to show one, you have agreements in place, at least with your key personnel, to protect confidential information. Two, you have handbook policies and IT policies that you give to your employees and train them on. Three, you have need-to-know restrictions. So not everybody at the company has access to all the information internally. Four, you have good exit procedures so that when somebody's going out the door, they're reminded about their agreements and you're making sure that they are at least being encouraged to return everything. Five, in instances where you're aware of violations, you know, you're sending demand letters, you're getting things back, you're suing when you really need to. Broadly speaking, those are the categories. And then you can sort of drill down on each one, and make it more sophisticated.

Rich Meneghello (10:12)
Okay. Where do you see, Michael? I mean, you obviously talk with employers all day long and you see this, and when you get a situation where they tell you, “Hey, we've got these trade secrets,” or maybe they're concerned that they've been taken by a departing employee or something like that, and you realize they've fallen short in terms of the reasonable measures to try to keep it secret, where do you see them most often fall short in that area?

Michael Elkon (10:34)
I think inconsistent enforcement, you know, having good policies in place, having good procedures in place, but then when you get into the actual nitty-gritty of it, they're not really consistent with applying them. I would say that. So, you know, you have really good agreements, but you don't have all your key people sign them. You have good exit procedures, but they're not enforced all the time. You have good IT training, but if people ignore it, they're not required to take it, things like that.

Rich Meneghello (11:15)
All right, the third thing, Michael, we want to talk about: the exit door. It's the highest-risk moment when it comes to trade secrets. So why is this stretch so dangerous for employers?

Michael Elkon (11:27)
I nickname these cases—this is not my own personal invention—these cases are nicknamed “business divorce cases” because they're like a divorce in a lot of ways, and one of them is that there's a lot of emotion associated with them. There's more emotion in these cases than there is in the typical employment case because somebody is choosing to leave one company and go to another, you can see the obvious parallels there to family law. And so the reason why this is dangerous is it's sort of a charged emotional environment. And so that sort of combination of self-interest and emotion will induce people to take trade secrets fairly frequently.

Rich Meneghello (12:15)
Right. We gotta keep it sports-related a little bit more, Michael. This is not a sports podcast, yet, exactly. But let's talk about another case involving sports, and that's a case involving the New York Knicks and the Toronto Raptors and the NBA. What happened there? That was interesting as well.

Michael Elkon (12:33)
So in in that case, the Knicks alleged that a video and analytics staffer was essentially recruited by the Raptors in June of 2023 and forwarded confidential files to his Gmail account and then to his Raptors email before he left in August. That was interesting to me for a couple different reasons. One is it's a similar sort of category of sports-related trade secret in that it's the sort of analytical IP that a sports team would generate analyzing players and teams.

And then, second of all, what was interesting about it is that forwarding emails to your Gmail account and then your competitors' email account is about the lowest-tech way to steal trade secrets. Like after bringing your secretary in to print documents, the next iteration of trade secret theft was “I'm gonna send things to my Hotmail account” because we're talking about 2006 here. And so people would do that. And that's really the easiest thing to catch. Like when I counsel clients on a situation where a key employee has left, what I'll usually tell them is, let's take their computer and any devices that you issue to them and get that off to a forensic expert so they can tell whether this person was using thumb drives or the cloud or sort of sophisticated ways of taking things. But what you can do in the intervening period is just look on their Outlook because you're not changing any metadata by doing that. Just take a look in their Sent folder and see if there's anything interesting there. And not all the time, but some of the time, and this is probably how the Knicks caught this staffer, just looking in the Sent folder is enough to get something incriminating.

Rich Meneghello (14:22)
Any other places that you feel it's an easy place for employers to look to see if they could spot suspicious activity?

Michael Elkon (14:29)
I mean, depending on the sophistication of the IT department, if they have DLP tools or any sort of tools that would flag large downloads, utilization of cloud-based storage, that sort of thing. Most employers don't have the ability to track USB usage. That's usually something that we have to get a forensic expert involved in, but the more sophisticated clients can look at that. But I mean generally speaking, you're just looking for evidence of information leaving your system.

And companies have gotten better and better at that. I mean, it sort of dovetails with their data loss policies in place that they've gotten good at figuring out when information has gone out of the system. And you know, so the same things that you're doing to ensure that you're not having some sort of privacy breach, you're also doing to make sure that your employees are not taking things.

Rich Meneghello (15:28)
You're listening to the FP 5. I'm Rich Meneghello, and we're here with Michael Elkon, a partner in the Fisher Phillips Atlanta office and co-chair of our Employee Defection and Trade Secrets practice group. You can find links to all the Insights we're discussing today in this episode's show notes.

So, Michael, let's jump to thing number four, and that's not just watching the door as employees are walking out of it, but watching the front door too as new employees are coming in.

We've seen situations where employers can end up as defendants when employees who are arriving as new workers bring trade secrets with them and then somehow bring a new employer into a web of trade secrets litigation. So how does an employer end up as a defendant in these kinds of cases that you've seen?

Michael Elkon (16:20)
Employers are often brought into these cases. Sometimes they're brought in when they haven't done anything wrong and sometimes they're brought in when they've done a lot wrong. And you know, it's up to the litigation process to sort that out. Generally speaking, it's important for an employer when they're hiring from a competitor to sort of think through "What is it that I would want my competitor to do if the shoe was on the other foot?" So you wanna obviously have them promise that they're not bringing any information with them, right? And you want to make it clear to them, like, "I'm not just talking about physical property. I'm not talking about 'have you returned your laptop and your phone?' I'm talking about anywhere that electronic information exists, I want you to make sure that you don't have any of it that would belong to your former employer." Right. So your Gmail, your laptop, your thumb drive, your external hard drive, your, your Dropbox, your iCloud, all of it. And then the question just becomes like how much do you need to verify what they're doing and how much of it is just "I've given them an instruction. I've told them the importance of making sure that they don't bring anything with them. Now it's in their hands and if they screw it up, that's on them."

Rich Meneghello (17:40)
There you go, yeah. Another article that is in our show notes. It's an older one, but it's still a good one: the Waymo case. Tell us about that one.

Michael Elkon (17:49)

Sure. I think about this one every time I get in a Waymo, which is pretty much only when I'm in Phoenix, because that seems to be the market where they're using them a lot. So there was a really famous trade secret case in about 2016, 2017 between Waymo, which was a Google spin off at the time, and Uber. They were competing to see who was going to come up with the first really scalable drivable, sorry—autonomous—car. And the key to having a functional autonomous car is LIDAR, which is the sort of the form of radar that a car uses, an autonomous car uses to detect what's in its surroundings: read red lights, see where cars and pedestrians are, et cetera. And so the star of the show in this case was a guy named Anthony Lewandowski, no relation to Barcelona striker Robert Lewandowski. And Mr. Lewandowski moved from Waymo to Uber and took a just an enormous amount of information with him. And one of the key facts in the case was that Uber didn't even have him sign an acknowledgement that he wasn't bringing anything from Waymo, even though it had other Waymo personnel moving to Uber sign those sorts of documents, which was something that the judge in the case noticed. So, in essence, Uber ended up in a lot of trouble because of A), the amount of information that Mr. Lewandowski brought, B), the importance of that information, like literally one of the most important pieces of information in a critical industry where whoever got to market first was probably going to be the winner. And then Uber not really doing everything that they should have to ensure that Mr. Lewandowski was not bringing trade secret information with him.

Rich Meneghello (19:57)
No trade secrets discussion could be complete without truly talking about the secret formula of Coke. And given the fact that you are also from Atlanta, Michael, we do need to talk about Coca-Cola. There was a Pepsi/Coke case, wasn't there?

Michael Elkon (20:16)
There was indeed. And this was a fun one. This was relatively early in my case or sorry, in my career as a trade secret litigator. So I found this one fascinating. I didn't get to work on it, but there was an executive assistant to one of Coke’s top executives who had this bright idea that she was gonna make some extra coin by selling Coke’s business plan or plans to Pepsi. And so she, I believe she worked with her boyfriend and her boyfriend's brother, if I'm remembering the details correctly. And the three of them ...

Rich Meneghello (20:50)
Sounds like Tanya Harding here.

Michael Elkon (20:53)
Yes. And it ended about as well for this woman as it ended for Tanya Harding. So they offered these business plans to Pepsi and Pepsi quite smartly reached out to Coke and said, “We just got the most interesting offer. We thought you should be aware of it.” And Coke then worked with law enforcement essentially to do a sting where they would induce this executive assistant and her cabal into essentially stealing trade secrets and then offering them to an undercover agent. The funny little detail on it was that the undercover agent paid thirty thousand dollars and handed it over in a Girl Scout cookie box at the Atlanta airport, which is where all business is done in Atlanta.

Rich Meneghello (21:41)
Do we know what kind of cookies the box was?

Michael Elkon (21:43)
Oh, I can only speculate.

Rich Meneghello (21:47)
I would hope Thin Mints 'cause those are the least suspicious, but okay. Wow.

Michael Elkon (21:52)
Yeah. Anyway, so that this led to criminal sanctions against the conspirators. They were arrested. They were all ultimately convicted. I believe the administrative assistant got eight years. Her co-conspirator got five. There were a couple of sort of key lessons about this. One was if you receive an offer the way that Pepsi did, it's always better to tell the competitor than to agree to accept the trade secrets. So that was a smart move on Pepsi's part. And second of all, it's an illustration of the fact that trade secret law has both civil and criminal components to it. So in the same case you can have both civil and criminal liability.

Rich Meneghello (22:43)
Which is a perfect segue to our fifth thing, and that's when things go wrong, you gotta get it right if you're an employer when it comes to what forum you're going to, whether you're gonna try to seek a court injunction, or whether you even maybe, like you said, bring in prosecuting authorities. Let's talk about the newest case probably that we as a firm have talked about and published about was in Massachusetts, and it made the process of getting an injunction, a court order, ordering somebody to stop doing something or doing something harder to get. What happened in that case?

Michael Elkon (23:18)
Sure, that's the Daikin case. Am I pronouncing that right? Is it “Day-kin” or “Die-kin” do you know?

Rich Meneghello (23:25)
I don't know, Michael. Let's just call them “the employer.”

Michael Elkon (23:29)
Okay. The employer brought trade secret allegations against two of their former employees for taking information, contacting customers, starting a competing business, et cetera. And the Massachusetts Supreme Judicial Court said that they did not see irreparable harm there, and that you have to have irreparable harm in order to get an injunction. And that in this case, they did not see that possibility or that likelihood because this was a situation where we're talking about lost customer relationships and therefore they could be made whole by money damages.

So it's representative of what I think is a larger trend. Our firm tracks trade secret, restricted covenant, duty of loyalty decisions sort of on a daily basis through Blue Pencil Box. And the daily alerts from Blue Pencil Box seem to have an increasing number of cases where either state or federal courts are saying, “I'm denying this request for injunctive relief for lack of irreparable injury because I think you could be made whole by money damages. Therefore you need to litigate this like a normal money damages case.”

Rich Meneghello (24:47)
As we are wrapping up this episode and talking about the way cases can end up, let's tie up some loose ends and talk about a few of the cases we've been talking about and how they actually ended up. So let's talk about the Knicks/Raptors NBA case. How did that case end?

Michael Elkon (25:03)
The Knicks sued in federal court. They were seeking more than $10 million in damages. And then it was sent to, I believe, arbitration. The NBA has a set procedure in place where cases need to be, I believe, resolved by the commissioner. The whole objective there is it's bad for the NBA, or any pro sports league, if your teams are suing one another in court. So it was ultimately resolved, I believe, by Commissioner Silver, and I don't know what the ultimate resolution of it was.

Rich Meneghello (25:40)
Because they haven't revealed it.

Michael Elkon (25:42)
Correct. Which may in and of itself be a trade secret.

Rich Meneghello (25:48)
Yeah, there you go. Exactly. What about the Waymo/Uber case? How did that one wrap up?

Michael Elkon (25:54)
That one did not wrap up very well for Mr. Lewandowski. Uber ended up settling it for, I believe, $245 million in 2018. So I mean, needless to say, these were some valuable trade secrets. Mr. Lewandowski pled guilty to one count and he was sentenced to 18 months in prison, he was fined $95,000 and had to pay $750,000 in restitution to Waymo.

And then in one fun little trade secret twist, he was pardoned by President Trump in January of 2021.

Rich Meneghello (26:30)
Do we know why?

Michael Elkon (26:32)
I could only speculate.

Rich Meneghello (26:34)
Well there you go. Last thing before we wrap up this part of the podcast. When should an employer think about bringing law enforcement in instead of just going to court?

Michael Elkon (26:42)
That's a good question. So the default I think with law enforcement, I'm just basing this on my experience, is that law enforcement generally view most trade secret disputes as a civil matter, as a matter between employer and employee and second employer.

So the kind of situations where law enforcement will get involved would be if you're talking about an especially important piece of trade secret information that's taken, right? So Uber/Waymo LIDAR research would fit. If the facts are especially egregious, if there's some angle that makes it different than a normal trade secret case, is there a foreign government potentially involved? Are there federal statutes involved? Something that takes it out of the normal realm of what judges see in terms of day-to-day trade secret matters. And then last of all, I often tell clients that if law enforcement is your end goal, than litigating a case in a civil context and proving your claims

through discovery and doing all the work that the Department of Justice would have to do on its own if it was starting the case from scratch. That can sometimes be a way to get law enforcement involved. If you show up on their doorstep with this nice case with all the evidence they need wrapped in a neat little bow and you hand it over to them, they're more likely to run with it, because you've done the hard work for them.

Rich Meneghello (28:19)
Well, okay, Michael, before we let you go, this is the part of the show where we get to know you a little bit better, let the audience get to know you a little bit better by asking five questions about you. Are you ready?

Michael Elkon (28:30)
I am as ready as I'll ever be.

Rich Meneghello (28:32)
All right, I know the answer to the first one because I know the answer to this, but let's tell the audience here. Which is your favorite soccer team and why?

Michael Elkon (28:39)
My favorite soccer team is Football Club Barcelona. I have been a fan of theirs since 1997 when they had the Brazilian Ronaldo. And I backpacked in Europe and it was my favorite city I ever went to.

Rich Meneghello (28:53)
You are a bit of a Euro snob, in a good way. In a good way, I'll say.

Question number two, what's the most interesting book that you've read recently?

Michael Elkon (29:01)
Most interesting book I've read recently was *Fear Itself* by Ira Katznelson about the congressional coalition that passed the New Deal. It was very interesting; it was essentially Northern Democrats, Southern Democrats, and Republicans. And then what FDR did to sort of put various parts of the coalition together depending on what they were trying to pass.

Rich Meneghello (29:30)
Yeah, okay. I know we could probably just do a history podcast with you and you'd probably nerd out even more than we have about trade secrets, but ...

Michael Elkon (29:38)
I could do a whole bit about the passage of the Fair Labor Standards Act and we could tie it in.

Rich Meneghello (29:43)
Oh gosh, okay. Let's avoid that. We don't want to put people to sleep too much.

Question three, Coke or Pepsi?

Michael Elkon (29:51)
Well, I've lived in Georgia for most of my life, so I will go with Coca-Cola.

Rich Meneghello (29:55)
You have to, right? You would get kicked out of the state perhaps if you'd answered differently. That was a litmus test. Good work.

Michael Elkon (30:01)
They would double my tax rate.

Rich Meneghello (30:03)
Fourth question. I know we're past the season, but I'm just curious now, what's your favorite Halloween costume you've ever dressed as in your life? And this is a PG podcast, Michael, so keep it clean.

Michael Elkon (30:18)
Okay. I'm generally not very good at dressing up. I did a good Mad Men once with like a three-piece suit and a fedora, although it turns out I don't look like John Hamm. So it wasn't a perfect one, but that's the first one that comes to mind.

Rich Meneghello (30:39)
Did you have seventeen drinks that day?

Michael Elkon (30:41)
Yes, it was just an excuse for me to drink.

Rich Meneghello (30:45)
It wasn't even Halloween, it was April.

Michael Elkon (30:48)
Yeah, every time somebody comes in my office, hand them a drink.

Rich Meneghello (30:52)
I recently finished a rewatch of Mad Men for about the third or fourth time and I really just started I mean, I know it's so cliche, but I really thought about the fact that literally every time somebody would walk into somebody's office they would pour themselves a drink. And it would be like ten in the morning sometimes.

Fifth and final question what would you do if you weren't a lawyer?

Michael Elkon (31:10)
Dovetailing back with what we talked about before, I would be a history professor.

Rich Meneghello (31:14)
I can still see it, I can still see it. You've still got time, I think, Michael.

Michael Elkon (31:18)
Yeah, I'd, my retirement dream would be to find a small town and teach a history class on World War Two.

Rich Meneghello (31:24)
Why a small town?

Michael Elkon (31:25)
Because I've lived in Atlanta for long enough, I'm gonna want something smaller, a little more bucolic, if I can use that adjective.

Rich Meneghello (31:34)
Sure. That's the first time that word has been used on an FP 5 podcast and with that I think it's time to sign off.

So Michael, thanks so much for being on the show. We really appreciate it.

Michael Elkon (31:44)
My pleasure. Happy to do it.

Rich Meneghello (31:48)
And thank you all for listening to the FP 5. You can find links to all the trade secret Insights that we talked about in the episode show notes. And we'll see you next week.

Listening to this podcast doesn't constitute legal advice and it doesn't establish an attorney client relationship. For more information, visit fisherphillips.com/legal-notices.