# **Trade Secret Law Evolution**

# Episode 57

## **Greenberg Traurig**

#### Speaker 1 (00:00):

This podcast episode reflects the opinions of the hosts and guests and not of Greenberg Traurig, LLP. This episode is presented for informational purposes only, and it is not intended to be construed or used as general legal advice nor a solicitation of any type.

#### Jordan Grotzinger (00:18):

Welcome to the Trade Secret Law Evolution Podcast, where we give you comprehensive summaries and takeaways on the latest developments and trends in trade secret law. We want you to stay current and ahead of the curve when it comes to protecting your company's most valuable assets. I'm your host, Jordan Grotzinger.

#### (00:37):

Welcome to episode 57 of the podcast. Back with me today is my partner, Greg Bombard, who is a shareholder in our Boston office, and our subject matter is going to be a little different today. As you know, our bread and butter, so to speak, is developments and case law. However, this past week we attended a seminar put on by global IP strategy hub called Trade Secret IP Protection & Litigation. And we had some interesting panels. Greg and I both hosted one with some very interesting people, including mostly in-house counsel that deal with trade secret issues. So we thought that it would be valuable to share some of the discussion points and takeaways that we learned from this valuable conference. I flew from Los Angeles and Greg, of course we met for dinner. It was too late to get the dinner at Contessa. Although by the way, David emailed me this morning and we're working on your holiday party at Contessa in January.

Greg Bombard (01:49):

I can't wait.

Jordan Grotzinger (<u>01:50</u>): So for you, Boston-

Greg Bombard (<u>01:50</u>):

You're all invited.

Jordan Grotzinger (01:52):

We have got to hookup. Greg, let's talk about your panel starting with the first subject, which partly overlapped with mine, which is the ongoing debate over the wisdom of cataloging or listing trade secrets.

Greg Bombard (02:06):

Yeah. Thanks Jordan. I thought really cool about this seminar, the conference. What I thought was really cool about the conference was the ability to exchange ideas between outside counsel and a significant number of in-house lawyers from IP departments in biotech companies, in tech companies, in computer hardware and networking space. So just a very broad range of perspectives and not just the perspective of in-house counsel on a particular case or your colleagues who are all outside counsel. It was great to have that diversity of thought and experience to talk about these issues.

# (<u>03:02</u>):

And one of the things that really resonated over these two days at this conference was this debate over whether it's a good idea whether you should attempt to undertake a catalog of a company's trade secrets. So you had on one side of this debate, a relatively vocal group of primarily vendors. People who are either will sell you a product to manage and track your trade secrets, sell you an audit or an internal process to identify your trade secrets, sell you an insurance product for the trade secrets. And those people were strongly advocating that you can't know what the trade secrets are unless you have a list, unless you've done some intentional process to identify what the trade secrets are. And that you can't take reason. You don't know if you're taking reasonable measures unless you have taken up a process to identify what the trade secrets are.

### (<u>04:17</u>):

And then you have the supposing view that I would say is led from two different groups of people who have a different perspective. And you have the in-house counsel who are managing the cat herding. The outside counsel perspective is I don't ever want to be in a situation where I am asserting a trade secret, and in a case. And the defendant says, well, this alleged trade secret is not on your company's official trade secret list, so therefore it must not qualify for trade secret protection. And that's a legitimate concern maybe. There was some debate in the room about whether that's ever been successful as an argument. And no one, at least in the moment seemed to know one way or the other.

#### (<u>05:06</u>):

And then the other concern really I think is practical. It's from the in-house counsel perspective. The cat herders who are going to be charged with maintaining or updating this list. And I think the perspective there if I was reading this right, is it's just not practical that you're never going to have a perfect list because your trade secrets are changing. The minute you finish the list, someone in R&D has created something new and it's not on the list. So it's never going to be up-to-date.

#### (<u>05:40</u>):

We also heard another interesting perspective was from Judge Young, who anyone who's practiced in the district of Massachusetts knows him. He's been a judge for a very time and is just this legendary federal judge in the District of Massachusetts. And he was describing how in his cases he would require a plaintiff to specify its trade secrets. And I've heard him use this quote in other contexts with the exquisite detail of a patent claim in order to get relief. And I thought that was interesting because that really speaks to this issue that it is of course difficult to, at the beginning of a case know what the particular asserted trade secret is because often the plaintiff doesn't know exactly what the defendant has done.

#### (<u>06:36</u>):

But Judge Young's perspective is if you're seeking relief in an IP case, you should be able to describe the trade secrets with the same detail you would in a patent claim. So that was one issue that got a lot of debate at the conference. And Jordan, do you want to react to that or do you want to talk about-

Jordan Grotzinger (<u>06:54</u>):

Yeah. I actually think that Judge Young's feedback about requiring this exquisite detail of a patent claim, which is really quite a standard. To me, that informs the question of do you need a list of your trade secrets. Because Judge Young is obviously talking about the context of litigation where you are fighting over particular trade secrets. So it makes sense in that context to identify them specifically. And of course we've had probably dozens of episodes of this podcast where we've addressed probably the most pervasive issue in this area, the issue of trade secret identification.

### (<u>07:49</u>):

So to me, for what it's worth and probably not worth much, I don't have a position that you absolutely should or shouldn't keep a list of trade secrets. To me it seems to be a function of timing and context. All of the naysayers on keeping a list who rightly believe that perhaps it's impractical because assets might be a trade secret or might not be a trade secret one day, and then be a trade secret the next day. Because of course, as we've also discussed a lot, a trade secret is something that's actually secret, valuable to your company and your competitors because it's secret and subject to the company's reasonable efforts to maintain its secrecy.

### (<u>08:43</u>):

A particular innovation or particular material might not meet all those three prongs through the life of its existence. And I would think that's the case for a lot of assets across a lot of businesses where a piece of information or a particular innovation might start as a non-trade secret but become a trade secret, or it might start as a trade secret and then lose that status because it can no longer meet one of those requirements. And that practical reality, I see how that can weigh against, well, why keep a list?

#### (<u>09:26</u>):

On the other hand, there are times and contexts in which you have to, for example, if you're litigating a trade secret case in front of Judge Young or a judge with similar requirements. And just lastly on this point, there was some concern on the bearish side of whether to keep a list that, well, you don't want a list to come back and bite you because it's binding and then you can't say later, well wait, I also have this other trade secret, but it wasn't on the list. And that speaks to the concern I raised at the top of my comment that materials and innovations evolve and might be a trade secret one day and not the other.

### (<u>10:15</u>):

I do think as somebody expressed, I believe on my panel that that concern can be allayed by a simple clear reservation of rights. If for whatever reason you feel you need to make a list of trade secrets, you can always make a record on the list itself elsewhere. It doesn't really matter where, as long as you've confirmed it. That this is not exclusive and it might be supplemented and there might be additional trade secrets that have to be added to this list. And if that's the case, I think it significantly diminishes the risk that a list could be used to limit the trade secrets over which you are litigating.

### Greg Bombard (10:59):

I think there's also maybe a goldilocks in between these two things where the parties aren't entirely talking past each other. The litigators don't want to be trapped into some position and the pro list people don't want there to be no knowledge of what the trade secrets are. But those are both two very extreme positions. And I think when we talk about what the reasonable measures that clients can use to protect their trade secrets, we often talk about a very standard sounding list of things. And this was something that came up over and over again over the two days. Talk about anyone who touches confidential information needs to be subject to a non-disclosure agreement of some kind, whether it's an NDA for a third party or some employment agreement for your employees, implementing technology controls like password protected laptops. Those things are the baseline.

### (<u>12:03</u>):

But once you get above the baseline, once you're trying to create a more custom solution for a particular industry, a particular client, you have to know, the lawyer needs to know what the trade secrets are. Because if it's a biotech company and the trade secret is some specialized method for cooking sales then that's just going to exist in a different form and it's going to be touched by different people and it's going to be used in a different way than the source code for some firmware system. It's just different. It exists in a different form, it's used differently, it's updated differently.

### (<u>12:48</u>):

So to some extent, we do need to be having those conversations with not just the lawyers. We need to be having those conversations to implement a good trade secret protection plan. We need to be talking to the scientists and the engineers and the subject matter experts to ensure that we're understanding what we're trying to protect. Because if you come at it with a one size fits all policy or solution, you run this other risk, which is that your solution is not tailored to the actual technology that the company is trying to protect. And that seemed like people could agree about that. We have to know we should have a baseline of what we're trying to protect before we start talking about appropriate reasonable measures because it'll differ depending on the situation.

## Jordan Grotzinger (<u>13:41</u>):

Agreed. And at the same time, in my experience anyway, it's very rare that you see, for example, a confidentiality agreement as part of someone's employment that specifically identifies trade secrets. Usually those tend to be written with a broader brush. But like I alluded to earlier, if you get to the stage of litigation, you've got to be more specific than what the confidentiality agreement says and identify the trade secrets with reasonable particularity.

### (<u>14:19</u>):

And just broadly speaking, and we addressed this on my panel and I believe at yours too. In terms of reasonable measures, to me, I've always looked at it like there are three primary buckets from which you can get protection. And those are technology, contracts and policies and physical barriers. The last one is less relevant these days. And as I said on my panel, my view is that the order of importance of those three buckets today in 2023 is probably the order that I just said. Number one, technology, number two, contracts and corporate policies about non-disclosure and number three, physical barriers. I mean, certainly you don't want to leave your office unlocked or your building unlocked if you've got technical documents. But these days they're stored electronically.

### (<u>15:22</u>):

And the last point I'll make on this, someone on my panel said, well, if a putative bad actor gets around a technological barrier, doesn't that necessarily mean it wasn't a good enough measure to protect the trade secrets, because the bad actor got around them. And as we discussed and as the law says, the answer to that question is no, because the standard is not a perfect measure to protect secrecy. It's a reasonable measure to protect secrecy. And you can see the sense in that law if you look at an extreme example of a hacker. If a sophisticated hacker manages to get through firewalls and breach technological security and field data, they should not be rewarded for being a good hacker, rather, the law says if the protection was reasonable, that suffices. It doesn't have to be perfect.

### Greg Bombard (16:40):

I liked the analogy that the car thief defense that you left the keys on the seat, not a very good defense. And it's a good reminder that in these cases, the lawyers can get very fixated on the technical minutiae of the law that yes, you have to prove as a plaintiff that you took reasonable measures to protect the secrets. As a defendant, if one of your primary defenses is that the plaintiff failed to take reasonable measures because they didn't limit access to the right people. And that's how I was able to get access to it. So I took it. That's not a particularly compelling defense when you really get down to it, because it seems to suggest that the defendant took the information, maybe even knew that they weren't supposed to take the information, but was able to circumvent the measures.

# (<u>17:46</u>):

It's not a compelling argument to be fighting on as a defendant. So then if you play that backwards to if we're going to develop a really good trade secret policy, from a legal perspective, the most compelling arguments, and there's data on this, there's law review articles on this. The most compelling element of a trade secret protection program for reasonable measures is just the existence of an NDA. And that by proving just that one fact, that controlling for everything else, proving that the plaintiff had an NDA of some kind in place with the actor who took the trade secret, the defendant, just proving that one fact increases the likelihood of success in a trade secret claim by orders of magnitude. And it dwarfs any other fact, physical security or whatever else.

### (<u>18:45</u>):

So it's easy from that perspective to say, well, all you need to do is have an NDA. But that's not the only thing. You're not just trying to win your claim. These other measures are there for a reason. You don't want to be a plaintiff in a trade secret case. So having these other measures in place, maybe less important on proving up your case, but they are extraordinarily important in avoiding having a case to begin with. If you make it difficult for your business partners to take your information at the end of the relationship, you're going to avoid having the litigation at all.

# Jordan Grotzinger (<u>19:22</u>):

And that, of course is the best case scenario for businesses. And one more thing to your point about the weakness of an argument that, well, I got through the firewall and therefore it wasn't a reasonable measure, that's a double-edged sword. And it's a dangerous argument potentially for a defense too, because as I believe you were suggesting, the more emphatically you say, hey, I was good enough to get through this, you just tip the scale on misappropriation on improper means, which is another thing that a trade secret plaintiff has to prove that the secret was taken by improper means.

### (<u>20:11</u>):

So a defendant arguing that, well, it wasn't a reasonable measure because it didn't stop me. That's a really risky argument because it can be used by the plaintiff to say, "See, he or she did this intentionally and willfully." So not only was it an acquisition by improper means, but it was willful, which as you know, Greg creates the risk of an attorney fee award and double damages as well under the Trade Secret Acts.

### Greg Bombard (20:45):

Yeah. Definitely not something you want to stumble backwards into. One interesting perspective that we heard over those two days was suggestions from the in-house perspective on ways that they were able to get buy-in for improving trade secret protection programs in their own companies. And we heard from a few people on my panel who were successful in getting business buy-in to improve the protection plans that were in place. And they listed a few factors.

### (<u>21:22</u>):

One was some element of scare tactics talking about the very large damage awards that you see from time to time in trade secret cases, including some of the recent ones that were in the billions of dollars.

Talking about just the sheer cost of litigation. And you can pull statistics on this stuff about the average cost of IP litigation from in-house counsel surveys. The problem with all of that, of course, and this is highlighted to great kemetic effect by some folks on my panel, that the problem is if you are the person who's just always predicting zombie apocalypse, and it never happens, then you just start to lose credibility, which you can't as an in-house lawyer.

## (<u>22:18</u>):

So doing these things in steps, doing it in ways that are easy to implement and digest. And one example that was shared was if you're going to try to improve your standard form NDA from just the basic thing that somebody found on the internet that everyone's been using, you might have different tiers, you might have different concerns for different types of counterparties. But if you try to implement some system where legal is reviewing every single NDA that gets signed, it's just too burdensome and it slows things down too much. So they won't do it. Your marketing people just won't do the thing you're asking them to do and you lose credibility.

## (<u>23:04</u>):

So one of the ideas that was shared is you have a standard NDA and then you have riders or codicils or whatever exhibits to this thing that have different covenant. It depends on the type of company we're dealing with. And it would have covenants in place for what the example we were talking about was imposing restrictions on vendors. If you're going to share your confidential information with a vendor, then depending on the vendor and depending on where in the world the vendor is, depending on what they're going to be doing for you, how involved they are, and how confident you are in their protection, their own protection of your information, you might impose more levels of scrutiny. But of course you can't take...

## (<u>23:55</u>):

In my mind, I'm imagining you have five of these. You can't take exhibit A five, the most restrictive one and use it for every single vendor because it's just ridiculous in some instances. So having that flexibility, I thought it was a great idea. You have different, they're just in the can and you're ready to dial up and down the level of intensity that you need for protection depending on whether you're just having an initial meeting with this person, whether it's M&A type situation, whether it's a vendor who's going to be producing material for you. Those are just different scenarios and you might want different protections in each of those.

### Jordan Grotzinger (24:34):

And I think it's important for an in-house lawyer to sell the proposals the right way so you're not, as you said, talking about a zombie apocalypse or being a harbinger, rather, your comment reminded me of one of our brother Brian Duffy's philosophy of optimistic urgency, right? Yes. Our business is one of problems, often scary, expensive, complicated problems. And it's very important how you approach that. And I think, although I've never been in-house, that the same holds true for an in-house lawyer who's trying to sell reasonable protections to the business people, who just want to do the business.

### (<u>25:26</u>):

And if you can sell it in a way that, hey, we're in the business of innovation and growing and providing the solutions we sell, this is going to make it easier. This is going to make it so that we don't have to worry that six months from now there might be a need to chase someone because they're out in the market using our secret stuff and harming our business. So really it's just all part of the protection and growth and development of the company and doesn't have to be sold as an impediment to a deal. Sure, it's a little annoying. I'm sure a lot of the business people don't want to hear it and they just want to

negotiate and do their deal without the right documentation. And of course, that's largely why we have jobs, Greg. And a lot of businesses at the same time.

# (<u>26:26</u>):

I'm sure with all due respect to us, wish our jobs were not necessary. So to make them less necessary, you've got to have reasonable protections. So I think it's important for in-house counsel to sell it the right way. I'm on your side, I'm part of the business solution, not an impediment. This is not going to derail the deal. Let's just [inaudible 00:26:49] the I's and cross the T's. So we're doing this right. We don't have a loss later.

# Greg Bombard (26:55):

And one last thing that came up on our panel that I thought was interesting because it's a topic that doesn't get a lot of attention at this conference. Usually at a trade secret meeting conference panel that you attend, you hear a lot about how do we protect the company's trade secrets from departing employees? And that's the basic trade secrets 101. The thing that we heard more talk about over these two days than I think I'd ever heard at one of these things was how do I protect my company from being tainted with information that comes from an employee that we're hiring. Or how do I avoid cross-contamination in a partnership? And I have my R&D guys and then I have this partnership and the partner provides us confidential information, it makes its way to the R&D department and all of a sudden everything is just tainted with the confidential information. It's impossible to get out. So what do we do upfront? How do we be proactive to avoid that?

### (<u>28:07</u>):

I thought that was a really interesting. It's a perspective that as a litigation person, as a litigator, I have that perspective because I represent a lot of defendants. So I see the way one employee's mistake can then just snowball into litigation. Quite frankly if it had been caught by the plaintiff earlier, the whole thing could have been avoided. The hard drive, whatever it is, would've been returned and everyone would've learned their lesson and gone home. But even when there's cases where there's no nefarious intent at all, it's just literally a mistake. Once you add time and technology and the information gets mirrored all over the place and then other people get access to it or whatever, unscrambling that egg is just very complicated and expensive.

# (<u>29:11</u>):

So what I was taking away from this was that in-house council, a lot of whom were in IP roles at various biotech and tech companies. They're really thinking about this issue in a way that maybe had not been given that much attention before. People are concerned and thinking about how do I avoid being a defendant in a trade secret case because of all those zombie apocalypse things. Because it costs a ton of money to be a defendant and it costs even more money if you're an unsuccessful defendant. So that was an interesting in-house perspective from this whole conference. How do we avoid being the victim of being the defendant, being a victim.

### Jordan Grotzinger (29:58):

Right. Back to my three buckets, I think that issue largely falls in the contracts and policies bucket. You need to have the right policies and contractual promises from onboarded employees about not bringing over or using the trade secrets of another. And really onboarding could be, we could do five podcasts episodes just on that because it's a very important process for all the reasons you said. And also, like you said, of course it's better to catch it early, but I've seen plenty of cases where you do and it's still quite burdensome and inexpensive to unscramble that egg, so to speak.

## (<u>31:00</u>):

Often if there's a, I'll say a rogue or sometimes the rogue doesn't even mean it. How many times does an employee just take a bunch of stuff from their other job and bring it to the new job, not because they had nefarious intent, but just because they want their form so they don't have to start everything from scratch? There's not intent to take trade secrets there, but they sloppily email themselves a whole bunch of data and forms and the IT folks at the prior employer find out, and all of a sudden you're in at least a \$20,000 dispute and negotiation with the new company about how to unwind that. And absolutely at least. Sometimes it can be up to 50 and of course if you get into litigation a lot more. So I think it's very important to have clear contracts and policies and other measures that we can discuss separately for onboarding purposes.

## (<u>32:07</u>):

So let's move on to my panel, which was on day two. The subject matter was prosecuting and defending trade secret claims. There was some overlap with the subjects on your panel and what we just discussed. The first subject was how does a trade secret case start? And the consensus answer was emotional. And I found that to be the case too particularly on the plaintiff side. You get a call from the client and more often than not in my experience, although I've seen it both ways, it's not about a discreet secret that's been stolen rather, it's about that data dump. IT sees that the day before a former employee departed, he or she emailed 100 documents or maybe downloaded or put in a Dropbox, a large volume of data and left. And then you get an emotional call or email from a client that may want to litigate right away.

## (<u>33:21</u>):

And another question that we discussed is what are the best practices to identify evidence of misappropriation when the client suspects it? You can't just run to court because the former employee in my example, downloaded a bunch of data. You've got a burden. You've got to show that there were probably some trade secrets misappropriated. And in my experience, what I've seen is that usually in my example, you've got to have the company IT folks, certainly you can offer third party or law firm IT help. But I usually have the company IT folks, if they have a robust IT department show us this data and I coordinate with the business people to identify, okay, of this cash of data, which materials are secret, valuable because of their secrecy and to you and your competitors, and subject to reasonable measures.

### (<u>34:28</u>):

The last prong is usually always met with a former employee because general... I don't remember the last one of these cases where the client didn't have an NDA. But you need to identify that at least some of the materials in that data dump will probably rise to the level of trade secrets before you run into court. And it's important to make that determination also because you don't want to waste \$25,000 on an injunction only to find out that had we looked a little harder, this data really wasn't that important and worth fighting over.

# Greg Bombard (35:06):

One thing that I thought was interesting about that question nor that comment about emotion is that another touch point for these cases is when there are multiple employee departures. And it seems common where you're getting the call either as on the plaintiff's side, or you're getting a call from a client who's been sued only after a group of employees has left. And the fact pattern often is you have this lead departure and some time goes by before that person is then joined by their team or key members of their team.

### (<u>35:58</u>):

And when the key members of the team leave, that seems often to be a triggering point for the further investigation then leads to this discovery of downloaded information. And I guess you could explain maybe on a broad brush why that could be the case. You can't run a forensic exam on every single departing employee's computer. So it's only when there's some reason for heightened scrutiny maybe that you end up doing those exams. But it's interesting because the employee rating non-solicitation angle of these cases is often the trigger point that then leads to a case that is potentially much more serious, that hiring away an employee, a non-solicitation breach is very difficult damages wise to prove that case as a plaintiff and quite frankly from a policy perspective can be difficult because there's strong public policy in favor of employee mobility. So punishing the employee who was solicited away somehow it seems just unfair.

## (<u>37:12</u>):

So what ends up happening is once the solicitations start to happen, that's when the trade secret misappropriation claims come out, and that's when the evidence of misappropriation potentially is uncovered. And maybe again having to do with your point Jordan, the just raw emotion that losing one employee is one thing, but being gutted of a whole team or a whole department can be much more emotionally fraught on the plaintiff side.

# Jordan Grotzinger (<u>37:42</u>):

Absolutely. And just as a matter of logic, the more employees and data that depart, the higher the chances that somewhere in that data there is actually valuable secret material that's worth protecting. I'm loving this episode so far. I feel like we could go another 45 minutes, but unfortunately I only have 10. So I want to get through the rest of these subjects and maybe we do part two of this episode because frankly this is a lot more fun for me than the case law ones.

### (<u>38:17</u>):

The next subject that we discussed was what does it cost efficient strategy for pursuing trade secret litigation? And one of the subjects we addressed under that issue is defining a win with the client early. And that relates to my point about when there's a bunch of data that's taken, you can use the word stolen, maybe it was just a dumb act rather than a theft, but when there's a bunch of data that's taken, you often and depending on how large of a volume it is, you don't know immediately what's in it or what materials within that data rise to the level of trade secret.

### (<u>39:06</u>):

And that's why, as I said, you want to get with your IT and business people, and try to determine that to see if it's worth fighting over. And in conjunction with that, depending on the volume of data that was taken and the value of the data that was taken, defining a win with the client for example, is it just... I've had plenty of cases that resolved before litigation with assurances from the other side that you know what, I was just being dumb. It wasn't part of a plan. I never opened the files, I never used it, I won't use it.

### (<u>39:46</u>):

So maybe a win, depending again on the volume and value of the data taken. Maybe a win is prelitigation assurances or a certification under oath that the secret materials have been destroyed and not copied and won't be used. Maybe it's more important than that and you need to go get a preliminary injunction, which often results often not always in an early settlement. Maybe it's a vet the company type case which justifies going all the way to trial and getting a jury verdict. And again, that depends on the volume and value of the secrets at issue, but particularly given the emotion that is at play when these cases first start. Because whenever there's a theft, the victim is not happy and they want to do something about it, and they're not always thinking doing something about it. If you hire a law firm immediately, it's going to be a large bill. So you need to breathe, focus on what's at issue, how valuable it is, and come up with a strategy early. What's a win here?

## Greg Bombard (41:06):

That's really wise because I think there's a tendency at the beginning of a case, especially from the outside counsel perspective, to think about these cases as all being vet the company litigations and they're not. Not all. So the wisdom to start early in defining what is a success going to look like, something more specific than just we want satisfaction or we want justice, or we want to punish them. Those things you're never going to achieve.

## (<u>41:41</u>):

So defining those outcomes, really good... Clients who have been through the ringer before are probably more disciplined at this, better at this of knowing when at some point you're never going to really know what happened. There's only so much forensics you can do, and at some point you're just going to have to trust the other side as you said, and just get as much return of information and data as you can. And then at some point there's going to be some gap that you have to bridge with certifications and trust. And you want to narrow that gap as much as possible, obviously. Sometimes litigation is required to get there. But if you can get to that point where you then feel comfortable stepping across the gap with some trust of someone who you legitimately as plaintiff probably don't trust, because they betrayed the trust in taking information to begin with. But at some point, that's how you're going to get out of the case. Defining those goals early can really save a lot of headaches and money.

## Jordan Grotzinger (42:45):

It's funny, the trust issues you just mentioned and that balancing on how much we can trust and how much we can risk by trusting given the breach of trust that started the whole thing. That's actually, I don't know if you remember, it's one of the first conversations we had, I believe it was last summer. I was dealing with a trade secret case on the plaintiff side representing a big company. A small team had departed. I got the sense that it wasn't one of these things where there was an elaborate plan to steal trade secrets, but rather just a dumb, I'm going to take my forms with me type of case.

# (<u>43:30</u>):

And it really came down to, I don't know if this is worth litigating over when we can probably get assurances and what should the scope of those assurances be. So that was actually one of our first conversations. In any event, it just goes to the point that, this is the issue that you should discuss at the outset of a case with the client so that you're bringing value and you're not spending too much money on something that wasn't worth that investment and vice versa.

### (<u>43:59</u>):

I want to touch on two other issues that we dealt with. One was the role and effectiveness of motions to dismiss. We discussed two things. One, the common grounds of such motions and the consensus there which matched my experience was that those tend to be over the identification of trade secrets, specifically the insufficient identification of trade secrets. But the consensus also was that they are generally, and of course it's case specific, not worth it because unless you've got allegations in the pleading or facts that are subject to judicial notice that show that the material at issue actually isn't secret and is a matter of public knowledge and already used in the business, unless you've got a dispositive fact like that that you can use at the pleading stage odds are, the court's going to grant leave to amend. You're not going to land a knockout punch as the moving party and rather it may be

counterproductive because you're just focusing the plaintiff on its trade secret identification. So the consensus was, you want to look at it, you want to advise your client, they're usually not worth it.

## (<u>45:23</u>):

And the last issue, and I'm going to preview hopefully another episode that we're going to do. One of our panelists, I won't identify him by name, but the secret will be out if I can pull this episode off. He's the general counsel of an agriculture company and he was involved in a really fascinating case over the trade secrets theft of seeds, like literally seeds that you plant, and spies that were crawling through fields and digging up these seeds. And instead of civil litigation, they called first the local police, which not surprisingly is not going to jump in their squad cars and go handle the trade secret case. But the FBI got wind of it and it became a big story. So I am working with this general counsel to do an episode on that story because I think it would be fascinating.

## (<u>46:21</u>):

And with that, I'd love to keep talking. We obviously will do this again, Greg. But I've got two minutes and I've got another call. It's a pleasure to see you, man. It was great seeing you this week. I had a great time at the seminar. Thanks for pushing me to get on a plane and go to that thing because it was great to see you and all our colleagues and also develop some new relationships and learn something that I hope we have shared somewhat effectively today.

## Greg Bombard (46:51):

It was great to see you today. It was great to see you earlier in this week. And I got to say one of the best things maybe to come out of this conference was the extraordinary interest in the podcast. I just thought that was really great to see so many people running to sign up to subscribe. So maybe there's some first time listeners on this episode, welcome.

### Jordan Grotzinger (47:12):

I hope so. And one of the biggest reasons for the success obviously is our incredible producer, Catherine Heller, who I am looking at right now. All right, guys, great to see you both. I'll see you again. Bye everybody.

### (<u>47:28</u>):

Okay, that's a wrap. Thanks for joining us on this episode for the Trade Secret Law Evolution Podcast. As the law evolves, so will this podcast. So we value your feedback. Let us know how we can be more helpful to you. Send us your questions and comments. You can reach me by email at grotzingerj@gtlaw.com or on LinkedIn. And if you like what you hear, please spread the word and feel free to review us. Also, please subscribe. We're on Apple Podcasts, Stitcher, Spotify, and other platforms. Thanks everybody. Until next time.