Hiring to Firing Podcast — Beyond the Dream Heist: Inside Today's Corporate Espionage Threats
Hosts: Tracey Diamond and Emily Schifter
Guest: Evan Gibbs
Recorded: December 16, 2025
Aired: January 6, 2026

Tracey Diamond (00:00):

So today we have a special guest on to talk about corporate espionage and we're using the movie Inception for this episode, which is all about dreams. So it had me thinking, Emily, do you have a dream that you have, a recurring dream?

Emily Schifter (00:13):

I don't really have a recurring dream. I mean, I always have the wake up in a cold sweat at 2:00 A.M. worried about something that's going on every now and then. But what about you?

Tracey Diamond (00:22):

Other than the usual sort of cliche, I guess my dreams are really cliche, like taking a math or a science exam and a nightgown in the middle of an old drafty room, I would say I don't. And I remember you telling me that you're not a big fan of dreams. Is that right?

Emily Schifter (00:35):

I have a unique pet peeve where I cannot stand to listen to people tell long stories about their dreams. My husband will always say, "I've got to tell you what I dreamed about last night." And 20 minutes later, I'm like, "It's not real. Didn't need to hear it." I would be a terrible character in Inception.

Tracey Diamond (00:50):

Well, the dreams never really make a whole lot of sense anyway.

Emily Schifter (00:53):

That's right.

Tracey Diamond (00:53):

But this episode does make a whole lot of sense. And there's some really good tips here for employers to think about in terms of protecting their data and ensuring that employees don't come in with another company's data and that they don't exit with your data. So listen on in.

[INTRO]

Tracey Diamond (01:06):

Welcome to Hiring to Firing the podcast. I'm Tracey Diamond, a labor and employment partner with Troutman Pepper Locke, and I'm here with my partner and co-host, Emily Schifter. Together, we tackle all employment issues from hiring to firing.

Emily Schifter (01:28):

Today, we are thrilled to welcome as our guest, Evan Gibbs, who is one of our partners in the labor and employment groups. It's just down the hall from me here in Atlanta. And of course, was the esteemed prior co-host of this podcast. So Evan, welcome and we're glad to have you back.

Evan Gibbs (01:43):

Thank you. Thank you. I'm glad to be here.

Tracey Diamond (01:44):

So Evan, why don't you tell us a little bit about what you've been doing since you left us at Hiring to Firing?

Evan Gibbs (01:50):

Gosh, well, when I was still on the podcast, I guess pushing three years ago, I think, I started what's called the Corporate Espionage Response Team here at the firm. We handle exactly what it sounds like, corporate espionage matters. So there's about 20 people on the team at this point. There's a mix of partners and we're adding in some associates now, but we focus, we're from a bunch of different practice groups, from white collar to data privacy, our e-discovery attorneys, labor and employment business litigation. We come from, I think it's a total of six different practice groups. Geographically, we're spread out all over the country and we handle the investigations and lawsuits that come out of corporate espionage. And so for our purposes, our team, when we're talking about corporate espionage, we're talking about really the unauthorized sharing of company information for commercial purposes. In our context, that information is taken by an insider, which is, we consider anybody who's been given access to that data or those documents on a voluntary basis by the company.

So of course, a lot of times it's employees. That's the most obvious suspect, but it also involves other individuals like vendors or contractors who may come in to help some kind of project for the company and they get access and they end up taking things. We can also be sometimes state actors from other countries and they may get access through someone else or, we've kind of seen it all, all the kind of crazy scenarios you might think of, but it's usually the information is then used by a competitor, whether it's a startup, which is what we see a lot of times. We might see an executive leave take a bunch of stuff and then start their own competing company or

somebody may leave and take it to a well established competitor or they may share it, again, with like a state actor or somebody like that.

The motivations behind this are sometimes it's personal. They just really don't like the company. They want to harm them in the marketplace, hurt the company. But a lot of times it's really, they're trying to make out some kind of competitive advantage, either again, starting a new company or helping a competitor unfairly. So that's primarily what I've been doing. So that's probably, I would say at this point, that's 90% of my practice at the firm. So I do those investigations and lawsuits kind of all over the place. So it's been busy. It's been busy.

Tracey Diamond (04:19):

Evan and I have had the opportunity to work together on a couple of these cases over the last six months or so, and they move quickly. They're high profile, they're really important to the company, and they're super fun to be litigating.

Evan Gibbs (04:32):

Yeah, that's right. They are.

Emily Schifter (04:33):

It seems like everyone's talking about corporate espionage and trade secret misappropriation. I feel like I see it in headlines. I have clients asking me about it. Do you feel like there's a rise in the volume of these sorts of cases, Evan?

Evan Gibbs (04:44):

Yeah, we have seen that. One way you can tell, you can look at when you file a federal lawsuit, you have to fill out this little civil cover sheet and you have to check a box on there and basically you have to identify, you have to tell the court what kind of case it is. The federal judiciary, they track the number of cases filed under all those different categories and so you can look at the cases filed. For example, a statute we see a lot of is the Defend Trade Secrets Act. You can track those cases and you can see that the number of those cases filed has been on the increase for year over year for a long time. And then that's only federal cases in that one statute. And we see, of course, a lot of state court lawsuits and that doesn't even get into the number of investigations.

So the answer to your question is yes, I feel like I'm seeing a lot more of it. It's so much easier now. People have more access to more data and people themselves, the human beings are more decentralized than they've ever been. I think that really makes it much easier to steal stuff than it used to be. Now, on the other hand, I will say that our clients are also getting more sophisticated. And so while people are doing this more, I feel like we're catching more of it. I mean, I can't say that for sure. I don't have some case study or something to back that up, but it feels to me like more often now when clients come to us, we're able to really answer those questions. A lot of times pretty definitively of, we think this person took something and we can a

lot of times confirm it or say we really don't think they did, but we do. It does seem like there's more of it going on for sure.

Emily Schifter (06:18):

That's been something that's been so interesting to me when we've partnered on some of these is just how detailed and specific we can get with a forensic evaluation. And I think back when, when people were just starting to use technology with their employees, it was not everyone had a governance policy or was able to track or let people do stuff on personal devices, things like that. Maybe it wasn't as easy to prove that something was taken. I think it's interesting now how much more we can do and how much your team's able to uncover.

Tracey Diamond (06:44):

It really is a word of caution to executives or any employee that's thinking of taking data on their way out the door. You can be tracked and it can be found out. So be warned about that as you're leaving.

Evan Gibbs (06:55):

Yeah. No, that's absolutely right. I mean, a lot of times people will take stuff accidentally and then maybe they go to a new company like, "Oh, hey, I've got these slide decks of really helpful information." I'll say that the flip side of this too is companies have to be really careful that when they are hiring, the people are bringing this stuff into the organization, because if your company brings something into your company and uses it, even if you, the executives of the company or even their direct managers, even if people didn't know about it, the company, the new company can absolutely still be liable for that use to the extent it harms the former company or to the extent it unfairly helps this other company. So you kind of have to be careful both on the sending and receiving, so to speak.

Tracey Diamond (07:43):

Yeah. We often will write into offer letters, representation by the employee to sign saying that they understand that they are not to bring any confidential information from a prior employer into the new company for exactly that reason. I'm sure you guys do the same.

Evan Gibbs (07:57):

Yeah, that's absolutely right. If clients ask me, which of course they never ask me until it's too late, and then I tell them and they maybe fix it later. But I try to tell clients like that, that should be one of the most important things you put in the letter. I mean, it is so important and it shouldn't be just an afterthought like, "Hey, please don't bring stuff." I mean, it should be like in bold towards the top and should really, really make sure the employee fully understands what that means because so many times people create something for another company and they feel like it's theirs and so they keep it and then they use it later and they do that over and over again is what I've seen. But if you create something for one company and they are paying you to

create it is that company's property. It is not their personal property and people don't get that distinction or they bring stuff in and then we have all these problems.

Tracey Diamond (08:45):

So I think this would be a good time to introduce our movie. For this topic, we chose the movie Inception, the 2010 sci-fi movie written and directed by Christopher Nolan and starring Leo DiCaprio. DiCaprio plays Dom Cobb, a professional extractor who uses experimental dream sharing technology to infiltrate their target's subconscious and extract information from their dreams. In our first clip, Cobb explains why the dream state makes a person particularly vulnerable to a search.

[BEGIN CLIP}

Arthur (09:14):

In the dream state, your conscious defenses are lowered and it makes your thoughts vulnerable to theft. It's called extraction.

Cobb (09:21):

Mr. Saito, we can train your subconscious to defend itself from even the most skilled extractor.

Saito (09:28):

How can they do that?

Cobb (09:29):

Because I am the most skilled extractor. I know how to search your mind and find your secrets. I know the tricks and I can teach them to you so that even when you're asleep, your defense is never down. Look, if you want my help, you're going to have to be completely open with me. I need to know my way around your thoughts better than your wife, better than your therapist, better than anyone. If this is a dream and you have a safe full of secrets, I need to know what's in that safe. In order for this all to work, you need to completely let me in.

Saito (10:04):

Enjoy your evening, gentlemen. As I consider your proposal.

Arthur (10:11):

He knows.

[END CLIP}

Emily Schifter (10:12):

The movie centers around a particular project in which Cobb and his team are hired to do the opposite of their usual technique. They're tasked with implanting an idea into their target subconscious, performing this inception on Robert Fischer, the son of a client's competitor, to convince Fischer that his late father wanted him to dissolve his father's company. Let's listen to this next clip.

[BEGIN CLIP}

Saito (10:34):

Robert Fischer, heir to the Fischer Morrow energy conglomerate.

Cobb (10:38):

What's your problem with this Mr. Fischer?

Saito (10:39):

That's not your concern.

Cobb (10:43):

Mr. Saito, this isn't your typical corporate espionage. You asked me for inception, I do hope you understand the gravity of that request. The seed that we plant in this man's mind will grow into an idea. This idea will define him. It may come to change. It may come to change everything about him.

Saito (11:03):

We are the last company standing between them and total energy dominance and we can no longer compete. Soon they'll control the energy supply of the world. In effect, they become a new superpower. The world needs Robert Fischer to change his mind.

[END CLIP}

Tracey Diamond (11:20):

So then the team meets together to create a series of layered dream sequences to infiltrate the idea into Robert Fischer's mind that his father would not want him to follow in his footsteps. So let's listen to our third clip.

[BEGIN CLIP}

Cobb (11:34):

Subconscious is motivated by emotion, right? Not reason. We need to find a way to translate this into an emotional concept.

Arthur (11:42):

How do you translate a business strategy into an emotion?

Cobb (11:45):

That's what we're here to figure out, right? Now Robert's relationship with his father is stressed, to say the least.

Eames (11:50):

Well, can we run with that? We could suggest to him breaking up his father's company as a screw you to the old man.

Cobb (11:55):

No, because I think positive emotion trumps negative emotion every time. We all yearn for reconciliation, for catharsis. We need Robert Fischer to have a positive emotional reaction to all this.

Eames (12:07):

Well, try this, my father accepts that I want to create for myself, not following his footsteps.

Cobb (12:14):

That might work.

Arthur (12:15):

Might? We need to do a little better than might.

Eames (12:19):

Thank you for your contribution, Arthur.

Arthur (12:20):

Forgive me for wanting a little specificity, Eames. Specificity?

Cobb (12:25):

Inception's not about being specific. When we get inside his mind, we're going to have to work with what we find.

[END CLIP}

Tracey Diamond (12:31):

Okay. So those series of clips are super interesting, and I actually got to watch the whole movie again to prepare for this podcast. It's a great movie. It's so clever and complicated. In real life, of course, we can't use dream technology to infiltrate or exfiltrate a company's employee's mind. What techniques are you seeing employers use to exfiltrate their company's data or employees use to take the data on their way out the door?

Evan Gibbs (12:57):

I will answer your question, but I do want to say something that's very relevant to the topic. This was about three weeks ago. This is after y'all asked me to do the podcast and I don't know if you guys implanted this into my subconscious or what.

Tracey Diamond (13:09):

In the dream state.

Evan Gibbs (13:10):

I know, I'm really not kidding. I very rarely remember anything that I dream about. It's extremely rare for me to remember my dream. But three weeks ago, I woke up and I told my wife, I was like, "Oh my gosh, I just had an Inception dream. I had a dream within a dream." And I remember in the dream thinking, "No, this is a dream. I can wake up." Anyway, it was really weird.

Emily Schifter (13:32):

Wild.

Tracey Diamond (13:32):

And did it involve sensitive corporate data of some sort?

Evan Gibbs (13:35):

Yeah, I don't know. I don't know. It was probably nothing that interesting. Probably something pretty lame. But yeah, so the techniques that I see, we used to see a lot of times people emailing stuff to themselves. That's very 2010. People aren't doing that anymore. I mean, people know better than to do that. And now some people, they'll do the old delete it trick. "Well,

I can send it and double delete it and I'm fine." Well, not necessarily, maybe, but most systems, most Office 365 environments hold double deleted stuff. There's a setting you can change, but most organizations will hold that for 30 or 60 days. So you can double delete, but if we get there in time, we'll probably still find it and we will be able to tell that you double delete it.

Emily Schifter (14:21):

Which is extra suspicious.

Evan Gibbs (14:24):

Exactly. And we do see that from time to time. Then there's, of course, hard drives, we got thumb drives and external hard drives. People do that pretty regularly, and it can be difficult to figure out exactly what device. Typically, you can see on a computer, we can always see every single device that's ever been plugged into the USB ports on a computer. So we know if something's been plugged in, there's no way to hide that. It can be difficult to figure out what it was. Sometimes some devices will tell you this was a Sandisk external 120 gig hard drive or whatever, but that's not always the case. And sometimes you kind of figure out was that somebody plugging in their iPhone to charge it or their Android or something? So sometimes it's unclear, but you always know when something's been plugged in. It's so easy now to use a cloud-based storage platform like Box.com or Google Drive is another one.

But you can have that if your organization lets you get into your user Gmail from your work computer. I mean, you can just drag and drop files across. I mean, it's so easy. And that is very, very hard to detect when people do that. And you can't know for sure if you do a forensic analysis of somebody's laptop, you can't tell for sure if somebody did that. If somebody dragged a file from their desktop or some other folder into a cloud-based storage site. What you can tell is you can tell that people interacted with certain files. You can tell that they visited the website, but there's nothing that says, "This person moved this file from point A to point B." And so you have to use basically circumstantial evidence when you're doing that. Now, if someone, sometimes people make the mistake of moving stuff out of some part of an Office 365 environment.

So like SharePoint, ShareFile, any of those Office 365 tools, if you pull files out of there, often you can kind of see the stuff that's pulled out of there, but otherwise that's really hard to detect. Another thing that's pretty much impossible to detect is if people take, if it's possible, if whatever they're taking is capable of somebody like taking a picture with a smartphone, if they've got their own personal phone, they come in, they take a picture of their screen, there's no way to detect that at all. I mean, unless you've got a security camera that's watching them, you can't detect that. But that's usually not really, for obvious reasons, that's not really practical because a lot of times the data's so big, you can't really, a picture's not helpful. But in certain industries, it could be very helpful. And you can do a video and scroll through lines of code or whatever.

There have been some very creative people out there that have done it. So yeah. And there's also been, for example, people have come in, I've heard, this did not happen in one of my cases, but I read a case where this happened where there was pretty early stage startup and they had some kind of new AI technology and these guys came to them and were acting like they were pretending like they were investors and they're like, "Yeah, we want to invest in your

company, but we need to demo over the product." And so the guys said, "Okay, yeah, sure." And they were kind of young and naive and they didn't really know what they were doing.

And so they did a Teams or Zoom meeting with these guys and came in and started showing them the technology. And halfway through the presentation, somebody else joined from the other side and the guy forgot to change his Zoom name and they recognized his name as being like some high person at this other startup and they realized what was going on. But that's another way, it's like people can get into meetings and listen to stuff different ways. So there's a lot of ways that people are trying to get stuff out, but I would say the most common are USB drives and the cloud-based storage.

Emily Schifter (18:03):

So you mentioned, we can kind of tell from a forensic perspective what's been plugged into a computer and that you can maybe use some tools with Microsoft 365 or Office 365 to figure out if things have been deleted. What other techniques can you use to determine that an employee has taken something they shouldn't have?

Evan Gibbs (18:19):

It's a lot of circumstantial evidence. It's what you end up with at the end of the day. There's a lot of, they visited this website, this device was plugged in and these files were accessed. Part of this is so complicated is it's hard to convey to, for example, if we have an active litigation and we have to go to a judge and tell them, "Hey, this person stole stuff off of this computer." It's really sort of an art to be able to take the technology, the circumstantial evidence that you get from the technology and then explain it to a judge in a room, who has no idea what you're talking about, sort of explain like, "No judge, we're 99% sure whether they stole it." And so it's a lot of circumstantial evidence.

Emily Schifter (19:04):

Tell the story and then hopefully unlock the key to formal discovery where you might then get to request that an employee give you things like a screenshot or a video, things like that.

Evan Gibbs (19:13):

Yeah, that's exactly right. That's exactly right.

Tracey Diamond (19:16):

Evan, if all this is happening on the backend, what can companies do upfront to protect their data from being stolen in the first place?

Evan Gibbs (19:24):

Yeah. There are, I think we mentioned the onboarding letters. I mean, I think that's like table stakes. I mean, I think you absolutely got to be doing that. You got to make it clear and make it

important. And you've actually got to police that. And I think there are a number of software tools out there that can detect suspicious activity. So I know like CrowdStrike is one of the software tools and I am not endorsed by CrowdStrike, but I know that's one option that's out there. There are a lot of other software products that are similar to that. That's just the one that's the only name that I know. But there are a lot of products that will, for example, they will send an alert to the IT department and say, "Hey, this person's downloading a lot of stuff. You may want to ask them. Hey, this person just emailed 20 things to a Gmail account."

So there are a lot of things that companies' IT departments can detect if somebody's trying to really do something sort of nefarious. So that's one of the first things too is to talk to the IT group and figure out what they are doing, what they can do, and maybe do some training with the IT group so they know what needs to be escalated to the right people if they see that. But I mean, other than that, I mean, training people on what they can and can't do is also super important as well. And that includes everybody from your executives all the way down to your lower level employees.

Tracey Diamond (20:44):

What about from the documentation standpoint, documents to put in place to make sure employees understand and agree to keep data confidential?

Evan Gibbs (20:52):

NDAs, confidentiality agreements, I mean, those are really great. I mean, having something more than just like an offer letter that's sort of a one-sided instruction to an employee, either coming in the door or out the door, that's all well and good, but it's much better if you've got a contract where they agree they're going to keep this stuff confidential. And if you're doing one of those contracts, it's good to be really clear about what kind of stuff you're talking about to the extent you're able so that people know like, okay, I can't take these certain Excel files or these particular slide decks. This is stuff that is kept confidential. And that was one other point when we were talking about Tracey when you asked proactive things.

Another thing that people can do is try your best in your organization to label things as confidential or trade secrets because that comes up a lot of times in cases is a defense will be from someone who took stuff. "Well, I took it. Okay, you caught me." However, it's not confidential and it's not labeled confidential and everybody and their brother had access to this and it went to clients and it wasn't confidential. So making sure that stuff that is confidential is actually labeled and is actually treated confidential by the company. That's something else that's just super important.

Tracey Diamond (22:04):

So like password protections, physical security, locks and keys, that kind of thing, right?

Evan Gibbs (22:09):

Yeah, for sure. And also, if you've got a document management system, making sure that only people have access to the things they need access to. Unfortunately, sometimes we'll come in and there will be really no user controls around who has access to what files in an organization and kind of everybody has access to everything. And then it's a tougher case for us to say, "Oh, this is super top secret." When everybody had access to it and we don't really know what anybody was doing with it.

Emily Schifter (22:35):

So more than just a good business sense of, "Hey, let's keep our confidential information protected." But actually can hurt your defense if someone does steal something if you don't take those steps.

Evan Gibbs (22:45):

Yeah, absolutely. Absolutely. Because let me tell you, some things, if you're a lawyer that deals with this or you work in business, it's obvious, it's sort of self-evident to those who deal with this stuff like, "Well, clearly this stuff is confidential. My God, we've never let this out of the organization. We'd never let a competitor have this." But judges don't live in that world. They don't live in that world. They don't care what your documents are. You've got to prove to the judge that this was in fact confidential and it's got to be pretty persuasive. If you just say, "Well, Your Honor, it was confidential." I mean, there are going to be follow-up questions.

You've got to be able to articulate all the things that you did to make sure that it was confidential and all the ways that it did not leave your organization except for this one person who's a bad actor. And that's something that just unfortunately gets overlooked. And a lot of times clients come to us and like, "Oh, this person took something and it's so bad." And I'm like, "Well, who had access to it?" "Well, I mean, yeah, we send it to clients sometimes, but we know they're not going to send it anywhere." It's like, "Okay, well..."

Tracey Diamond (23:45):

It could be fatal to a claim. Isn't it a threshold issue whether the document's a trade secret? Yeah.

Evan Gibbs (23:51):

Absolutely, absolutely. And it becomes just something that's really hard to prove. How are you going to prove, if 100 people had access to this document and they all had copies of it on their laptop, it becomes almost impossible to really prove and convince a judge like, "Yes, this was actually confidential and a trade secret."

Tracey Diamond (24:10):

What about employees and executives who are leaving the company? Is there actions that the company should take at that stage to make sure that they're guarding against data theft?

Evan Gibbs (24:20):

Yeah, for sure. I think the most important thing is making sure that their access to the company's systems is all shut off immediately. So it's obvious, and I think every client that I deal with in these situations, they turn the email access off at the right point, but a lot of times they forget for whatever reason to turn off access to other systems. So for example, if you have a document management system that's outside of the Office 365 environment, sometimes that access doesn't get cut off and the person continues to have access to files even though they don't have their email. And so they can continue to access some really highly confidential information after they've left the company. And maybe it could be weeks, days, months before somebody wakes up and realizes, "Oh, this person still had access." So you want to make sure their access is cut off to everything as soon as possible.

And if it's somebody that's a really high value individual within the organization, you may not want to wait until their last day with the company. You may want to do it as soon as they tell you. And that's very context and fact specific, but that's something to really think about because you may not want to give them that two week window to take stuff. So consider that. And the other big thing is to make sure that you get the laptop back from them. I mean, pretty much everybody has a company issued laptop. And so a lot of times the system access gets cut off, but the person's laptop still totally works. And so even though they can't get into their corporate email account or to their document management systems or other platforms, they can still get to locally saved files on the laptop. And a lot of times, a lot of people, and it's very common, I hate to say I'm one of them, I'm way better than they used to be, but there's a lot of stuff on my desktop.

And I know a lot of people keep important files on their local hard drive. So getting those computers back as quickly as possible and staying on top of the people to send them back is also really critical. And if there's a way to remotely shut down their access, then you should, and then have them work with the IT department to get their personal files off the computer, because they're absolutely going to have some personal stuff they're going to want to get off. So just be prepared for that.

Tracey Diamond (26:36):

I sometimes see attention between clients that want to have a transition period with certain employees, so they want to be able to continue to give them access so that they can transition their duties. And then this concern about the potential for the employee to sabotage or steal data on their way out the door. I guess the only thing I can think of really to do is limit their access in some way if you really still need to give them some kind of access. Do you have any other thoughts about that?

Evan Gibbs (27:01):

I think that's the answer is you've got to figure out what do they really need access to during this transition period? Is it just email? Can they live with everything else? And then you got to think, yeah, this might make it more of a pain for them to transition out. But now we really are able to really very carefully monitor them on this sort of final stages. So yeah, I think that's about the only answer is just trying to figure out what can you really shut off and still be able to practically handle that transition phase?

Emily Schifter (27:32):

It's a great point. I feel like I often have clients who think that the transition's a good idea, but in reality, once you tell somebody they're out, they're not always as helpful as you'd like them to be. And so sometimes the better approach is just to say, "Hey, agree to remain available for questions, but you don't need to have access to anything and you can just tell us where things are."

Evan Gibbs (27:49):

Absolutely.

Tracey Diamond (27:50):

I 100% agree with that. I think oftentimes the clients think that they need more of a transition than they really need. And even if the employee's being cooperative, it usually doesn't take as long to transition them out as employers think it's going to take.

Emily Schifter (28:04):

We're all replaceable.

Evan Gibbs (28:06):

That's right.

Tracey Diamond (28:06):

So we have an employee that steals the company's data. Describe for us, Evan, the type of litigation that may ensue at that point.

Evan Gibbs (28:13):

Yeah. I mean, we typically, we do the investigation. We feel really confident that the person took it and that we can prove it. Then if it's important enough to the client, then we would file a lawsuit in state or federal court. And we typically would file in connection with that request for a preliminary injunction. And so we would ask the judge, "Hey, Judge, make this person..." For example, if we're talking about an employee, we may say, "Judge, enter a court order that says

this person cannot work at that company for a month or whatever while we sort of sort this out or find they can't work for them at all because they've stolen our stuff and we see that they've given it to this other company." Often in these cases, we also have restrictive covenants like non-competes and non-solicitation provisions. And so a lot of times in connection with the trade secret theft claim, we're also trying to enforce some kind of contract as well, but that's typically how it works and it goes really fast.

When you file a request for a preliminary injunction, the courts treat that as an emergency filing. And so you're usually in court. I mean, I think the fastest I've ever been in court was three days from the date. A judge said, "Be here in three days and basically put on all your evidence and show me why I should give you this injunction." The longest was probably, gosh, like two and a half weeks or so. So it just really depends. It kind of depends on the court's schedule, but it's fast. I mean, the courts sort of clear their calendar for these cases and will get you in front of the judge really quickly. So they move fast and yeah, that's typically... Then after that, once the injunction piece is over, it becomes just a normal lawsuit. Whether you win or lose on the injunction, the case will typically proceed all the way through a trial if you need to, but they often will settle Sometime after the preliminary injunction hearing.

Emily Schifter (30:02):

We talked a little bit in the beginning about why it's important for new employers to be proactive about making sure that they're not on the back end of one of these suits. Having language and offer letters and agreements, things like that. Sometimes I'll have clients say to me, "Well, my new hire signed an agreement saying they wouldn't take any confidential information, but what does that have to do with me as the employer?" What are the types of claims that you might face as an employer who's bringing someone on? Why is it so important to have those measures in place?

Evan Gibbs (30:28):

Yeah. I mean, if, for example, let's say that you hire a salesperson to come into your company and they brought with them not just a client list, but detailed client information like order, history, financial information, they bring basically everything about the set of clients that they would need to basically go in and compete competitively, price the products the best way possible, whatever. Anyway, they use the trade secrets to get the business and then the new company, the new employer who is the beneficiary of that work, they could then be sued for trade secret misappropriation. Now, you can put up a defense, "Hey, we company did not know that this was going on." But that defense is probably not going to fly." The company from which the information was stolen, I mean, they'll have a right to get back that money that was lost. They can prove that the new company was unjustly enriched or unfairly secured these profits and that they can absolutely get a judgment for those damages.

And so we see the trade secrets claims under state and federal law. We see tortious interference with business relationships or with contractual relationships and you see those types of claims. You see sometimes civil conspiracy claims, you see all kinds of stuff. There are a number of claims that can be brought in these circumstances against a company who receives information. It's really very important. It can be a very, very costly issue if it sort of gets out of control with real damages.

Tracey Diamond (31:58):

Well, this has been a really important message for us, our clients to hear, and we really appreciate you taking the time to come back to your roots here at Hiring to Firing, Evan.

Evan Gibbs (32:07):

Absolutely.

Tracey Diamond (32:07):

It's been a pleasure having you on. Thank you to our listeners for listening in. Shoot us an email, let us know what you think, and give us some ideas for some future episodes. Thanks for listening.