Speaker 1: [inaudible]

Speaker 2: Welcome back to the performance review podcast. Our guest today is Todd pickles, a former assistant United States attorney and current of counsel here at Greenberg Traurig. Todd is a white collar expert who represents clients in white [00:00:30] collar matters and investigations and conducts independent investigations on alleged violations of criminal and civil law. And I'm sure it does a host of other things. So Todd, just welcome to the podcast.

Speaker 3: Thanks. I'm happy to be here. I appreciate you guys promoted me to expert, but I'm glad to glad to talk with y'all.

Speaker 2: Exactly. Look, I mean, you come on this show, you become an expert, so we're, we're very, very glad to have you, uh, I wonder if maybe if you could start by just telling us a little bit about your practice

Speaker 3: Since I've been [00:01:00] at Greenberg, I've been involved in doing a series of investigations, both in terms of situations where a client is a victim of a potential crime or where there is a, some concern about whether or not there may have been some wrongdoing and also an in court, uh, quite often representing individuals and corporate clients with respect to ongoing prosecutions and investigations primarily with white collar crimes. Okay.

Speaker 2: So, you know, and you, you know, that we're, we're in the labor and employment, [00:01:30] uh, practice group, we practice, uh, L&E here in California. Can you give us just a sense of how just big picture, how white collar issues impact California employers?

Speaker 3: Sure. Yeah. So, uh, as you can imagine, anytime you have a situation where there's money and people working together that can often lead to situations where criminal aspects occur, for example, embezzlement or other types of crimes, [00:02:00] uh, oftentimes in the process of engaging in perhaps an employment investigation, you might come across allegations of criminal wrongdoing. So it's not as uncommon as you might think that an employment matter has a potential impact on a criminal case or vice versa.

Speaker 4: And that kind of goes to our point that we say a lot here is life happens at work and I guess crime happens at work too,

Speaker 5: Right? So

Speaker 4: What are some of the potential crimes or criminal issues [00:02:30] that employers should be cognizant

Speaker 3: Of, but there's a kind of a host of different categories or potential categories of criminal activity that can arise at the workplace. One fairly obvious one would be fraud or situations involving money, but you could have, for example, external fraud where

efforts are being made to defraud people outside of the company that could involve management, for example, engaged in alleged criminal wrongdoing. You could also have situations of internal fraud, embezzlement, [00:03:00] and that sort of thing. To the extent that the company is publicly traded, you can have situations involving potential securities fraud, whether it be disclosures, insider trading, or other aspects of the company's dealings that implicate the securities laws. Also in extent, any employers are in the healthcare arena. That's another common area where you see criminal employment overlap, particularly when it comes to submission of claims and of a false claims act brought either civilly [00:03:30] or criminally.

Speaker 3: Those are to some kind of general aspects of fraud as it relates to the business proceedings. And the other piece that I should mention is the extent you have a company that does overseas work, uh, and there's an allegation that perhaps brides are paid overseas that actually can be prosecuted here in the United States under the foreign corrupt practices act. So that's one big category where you could have an employment situation that suddenly morphs into some kind of a criminal [00:04:00] investigation, or at least the need to determine if there is a criminal issue that's percolating below the surface.

Speaker 4: We think of wage and hour issues and other types of misconduct that can lead to some sort of criminal conduct or criminal situation. One thing that comes to mind, maybe a background check banning the box via had any experience there.

Speaker 3: I do know that some, what looked to be, uh, kind of more purely employment issues [00:04:30] can actually have criminal consequences. I familiar that under California's labor code, some conduct can actually, uh, rise to a misdemeanor offense, uh, and other circumstances, uh, you could have, uh, workplace issues that morph into a criminal one. Uh, unfortunately there are instances of workplace violence and that can include situations where there is criminal prosecution that's occurring because of what happened at the workplace and are those circumstances. The employer may [00:05:00] be concerned about their own liability civilly, but also wanting to cooperate with law enforcement, particularly if they're a victim or an employee is a victim and cooperate there too. And another area that I should mention kind of in addition to the fraud situation I discussed. And then Phillip, as you mentioned, this kind of more employment focused issues is trade secrets.

Speaker 3: Particularly if companies have intellectual property or are involved in that area with competitors, it's not uncommon that [00:05:30] if there's an allegation of, uh, uh, civil, for example, trade secret misappropriation, there can be criminal prosecutions that arise. And in fact, here in California, we've seen a little bit of an uptick, particularly in the Northern district of the department of justice, prosecuting criminally allegations of trade secret misappropriation or TJ get theft that happened after there had been some civil litigation. So that's just another area where you might have this overlap between employment matters [00:06:00] that traditionally are handled on the civil side and then a criminal case or criminal investigation that can kind of pop up even after the fact.

Speaker 2: So it sounds like there are just an absolute ton of ways for people to get in trouble at work. Um, what, what are right. I mean, in addition to, you know, Philip and I practice mostly on like the civil liability side of things, but of course there's this whole other world, w what are some of the things that you'd recommend for an employer to, to mitigate [00:06:30] risk? And maybe we could just start, even with that first bucket of topics that you mentioned with general fraud as an employer, how would I go about doing that in the state of California or I suppose elsewhere?

Speaker 3: Yeah. So kind of one of the most critical aspects is going to be just making sure you have a really strong compliance program when it comes to, to the expenditures or how money is distributed to in the company. You want to have strong controls, strong audit procedures, those kinds of things [00:07:00] that you're really making sure that, you know, kind of what's going on and when it comes to the fiscal activities of the company and then, and some of these are going to be great, both criminally and civilly. And for example, having some kind of program in place that provides for whistleblowers or anonymous reporting. So that if there is an instance where someone within the company does, uh, perhaps go off the rails a little bit, you have a mechanism in place to allow that information to kind [00:07:30] of percolate up to who needs to, to hear about it so that the company then can react.

Speaker 3: And then, and this goes, without saying across the board, the more training you have to inform the employees of the significant consequences to any criminal conduct, and also this, the need to be good stewards of the assets of the company are really gonna probably be the best features you can have to build in to limit the possibility of one of these civil cases suddenly kind of [00:08:00] morphing into a criminal, uh, or at least the risk of criminal exposure. And I should say that that risk of criminal exposure can go to obviously the individuals who are involved in the alleged wrongdoing, but also the company can be held criminally liable, uh, with, with pretty severe consequences under the federal law and in certainly under California law as well. Yeah. Yeah. Got

Speaker 2: It. You know, certainly something to keep an eye on. You had mentioned as well, trade secrets being one of the bigger, sort of the big buckets in which you might face [00:08:30] some white collar issues. What are some things a company can do to protect itself as to that category of, uh, of issues

Speaker 3: You're going to want to protect yourself both as a potential victim of trade, secret theft, as well as avoiding situations where there's allegations that you as a company have acquired wrongfully the trade secrets of a competitor. And so for example, having kind of controls about to what extent employees can utilize any of their own, uh, electronic, uh, equipment [00:09:00] or devices at, at work, uh, having strong non-disclosure policies restricting to what extent employees can access from work, uh, external email accounts or Dropbox or other, other situations of them actually being able to physically remove data and information all in an effort to really try to limit to what extent a company is going to be a victim of traits or cause, so this isn't kind of in a rocket science and would apply to most corporate structures. [00:09:30] And then the other piece is if you're taking on, for example, new employees, and they worked at a competitor having very strong protocols in place to ensure that that employee is not bringing along

anything that could be considered intellectual property of the former employer, and perhaps having some kind of a review process as part of that onboarding, just to really guard against the possibility that there is any potential that someone that's coming into [00:10:00] the shop is engaged in trade secret theft that can then present potentially, uh, subject the company to exposure.

Speaker 2: One of the, the other things you mentioned in terms of the big categories of ways employers can get in trouble, specifically as those in the wage and hour space, those misdemeanor statutes. And, and I have to tell you, as I go through the labor code, those always give me pause, right? It is not just civil liability, there's potential criminal liability that attaches to some of these statutes. So w what's something, again, aside from, you know, perfectly [00:10:30] complying with every, uh, aspect of the California labor code, which I know is quite difficult, what are some things employers can do to protect themselves there?

Speaker 3: Well, there, I think, as I mentioned with respect to the general fraud and financial aspects to have a strong whistle blower protocol or policy in place and internal reporting to really encourage the situation that employee feels comfortable raising an issue. So it can be quickly and hopefully decisively [00:11:00] resolved efforts made. And as you mentioned, kind of general compliance efforts, a lot of times when you have situations that potentially can go from civil to criminal is where there's going to be strong evidence of tent to violate the law and kind of repeated instances of violations of the labor code. And so to the extent that as a company, you can nip things in the bud early on, uh, may not ultimately avoid some civil [00:11:30] exposure, but it's going to go a long way in lessening, the likelihood that you're going to get involved criminally, that would be a kind of an example of, you know, a little, an ounce of prevention being worth a lot more than just keeping yourself out of harm's way. On the civil side,

Speaker 4: Todd, some of the employers, they have anonymous reporting websites are kind of methods that they can report. Uh, does that help minimize some of the risks there? I know you mentioned that, just making sure they have an opportunity [00:12:00] to report some of these things and become potential whistleblowers of, of, uh, uh, criminal activity. I just want to know if the anonymity is something that could assist here.

Speaker 3: I think it definitely could, if it's going to make it more likely that people are going to feel comfortable raising the issue, right. And, and all of the, the situations, what you're really trying to do is determine, is there some wrongdoing and then quickly be able to move to, to [00:12:30] resolve that issue if people are uncomfortable because there's not anonymous reporting, they know they're gonna have to put their, you know, uh, next out to raise an issue. Then they may not be willing to do it. It goes unreported. And that's really where you get to situations that are going to raise the eyebrows of a law enforcement agency. If there's something that's been going on for a long period of time, it looks widespread. And so the anonymous reporting, you mentioned, if that's going to encourage people to come forward, then that's really going to be, I think, [00:13:00] helpful for a company to consider, to avoid any kind of criminal exposure down the road.

Speaker 2: I think one of the issues employers have to be concerned about is, is just relates to workplace violence itself. Could you, could you, I mean, cause obviously there's, there's all kinds of criminal and civil liability that, that attaches to that topic. What generally are an employer's duties in that regard and how, again, sort of keeping with my theme here, how can an employer take affirmative steps to protect itself [00:13:30] with respect to workplace violence?

Speaker 3: I think the, you are right that there's kind of the civil and criminal kind of are going to line up fairly well here. And from a employer's perspective, the minute you get any information that suggests there could be workplace violence, whether or not it's between coworkers or perhaps, you know, a domestic violence situation. And you're worried about that spilling over into the workplace as a, an employer, once you get that information, you have to be concerned about, to [00:14:00] what extent is that realistic? And then what steps can you take to mitigate? Do you need to Institute some policies to, for example, bring in security, do you need to, uh, enhance the existing security that exists at a facility to ensure that only those that are authorized to be on the premises can gain access to the grounds, those types of situations that would be considered reasonable to make sure that your workplace remains safe now.

Speaker 3: And this is I think a really good example of where you have the interplay between, you know, [00:14:30] a potential criminal act and then the employment side that you guys deal with, because that also raises a host of issues about, you know, the relationship between the company and the employees. Uh, to what extent are these kinds of changes are going to maybe implicate some HR policies or need for HR policies. And another big one I will say. And unfortunately, you know, we always reminded of this oftentimes and tragic ways is having some kind of active shooter training or protocol, just so everyone knows, you know, when [00:15:00] things do go wrong, if they go wrong, that the company is in a position to do whatever it can to ensure the safety of people under those circumstances, those are all really good areas that a company can react or be proactive. If there is a situation where a concern arises about a workplace violence of the employers,

Speaker 4: Nowadays they provide their employees with a computer, a laptop or some other device, and we could do a whole show [00:15:30] on just what employees should not be doing on those devices. Um, I'll leave it at that and let some of our listeners minds a wander, but I know there's some criminal statutes relating to computer and fraud. Can you kind of educate us on that?

Speaker 3: Yeah. So there's the computer fraud and abuse act. It's, it's often kind of called CAFA, at least that's the, the way a former prosecutors speak of it. It's the criminal statute under title 18 of the us code. That's the criminal code provisions under federal law and it [00:16:00] criminalizes essentially unauthorized access of computer devices. It was historically is actually passed back in the eighties, at least in part, the story goes and based on some congressional testimony and kind of reaction to, or at least acknowledging the movie war games with Matthew Broderick, uh, in the eighties and kind of the fear of teenagers kind of hacking into NORAD and, and, uh, you know, causing all kinds of mischief. But really it was kind of a serious acknowledgement

[00:16:30] that given the interconnectivity of, uh, computers and the ability of hackers to get in there and maybe get the crown jewels of a company or whatnot, Congress traded a federal statute that both has civil and criminal aspects to it.

Speaker 3: And, uh, and, and I'll tell you a little bit, I actually had a case, uh, employment related case with respect to a CAFA allegation and prosecution with respect to unauthorized access. But that, that is definitely one that I think employers need [00:17:00] to be aware of. Certainly under those circumstances and employer, you know, you're, you potentially are a victim of, of hacking, uh, or it could be an employee actually, who within the company, it doesn't always have to be kind of the, the person, a farrier, mostly located elsewhere. That's attacking in, it could be someone right under your own roof. That's involved in accessing without authorization the company's information. And if it's causing harm and there's [00:17:30] a financial aspect to it, then usually that's going to potentially rise to at least an actionable Plame under CAFA. And, and that's an area where I think companies need to be really vigilant, particularly as technology evolves and the ability to there this level of interconnectivity, I think just as is going to increase. And before we go

Speaker 4: Any further, and since this is the performance review, I'd like your review on the war game.

Speaker 3: No, I, I love that movie. It was a, I thought it was a, a terrific movie. And, um, [00:18:00] you know, I was aging myself a little bit. It was when I was a kid and watching, watching that thing was, uh, was a lot of fun and I've had a chance to show my kids the same. And I don't know if they love it as much as I do, but it's now become a family tradition, uh, with at least within my family.

Speaker 2: Well, and if you're a federal prosecutor and you're bringing a case under, under CAFA, I mean, do you have to say that the only winning move is not to play? I mean, I feel like you have to put that in your closing argument. Right.

Speaker 3: You know, and in that particular case, [00:18:30] I decided to go and play it straight. But now that you mentioned it, maybe I should, uh, I should, uh, try to do that the next time. At least if, you know, if I'm on the defense side and asked, you know, do you want to play a game? Exactly.

Speaker 4: One other in a more serious note. One other point I have to ask you about CAFA is it sounds like it starts with the employer's policies and handbook. If they have a strong policy stating that what is authorized conduct and what is unauthorized conduct [00:19:00] on the employer's computer laptop or other device, does that help with the capital analysis or doesn't help at all?

Speaker 3: No, it's, it's going to be an, in some respects, kind of the, the first place you're going to go as if it's an insider and determining whether or not you can even a case. And that, again, that's both civil or criminal, but I can tell you that I'm wearing a prosecutor's hat. That was one of the first things that we had to determine in the case, as we brought in our cafes, what were the policies? How well were they distributed? [00:19:30] Kind of

how strong were they in limiting access for only certain people and for only certain purposes. And so that definitely going to be an area where as an employer, you're going to want to make sure that you have a very strong policy in place limiting access, identifying, you know, who can do what, because if down the line that you have a situation of someone kind of running a mock, that's going to be where you're going to start. And particularly as a criminal prosecutor, that's one of the first questions [00:20:00] they're going to have. If you're working with law enforcement to try to remedy that kind of a situation, and we've

Speaker 4: Talked about just authorization and getting access to certain systems on the computer. What about deleting files? I had situations where a client may have had an executive who's leaving and decided to raise certain things from, from the computer

Speaker 3: You think of hacking as kind of stealing or obtaining information. And then that's not necessarily the case under [00:20:30] CAFA and vendor trade, secret theft. That might be true, but when it comes to CAFA, just any kind of unauthorized access that is intended or kind of recklessly caused damage to a company is potentially actionable. And so kind of given the hypothetical, you mentioned the disgruntled employee on the way out the door, wanting to kind of, you know, not just burn the bridge, but, you know, burn down the, the company that could still rise to the level of a violation of CAFA know provided all of those, those elements are met. [00:21:00] I should caution that, uh, one aspect of CAFA is actually being litigated this term before the Supreme court. And it has to do with, you know, what does unauthorized access mean? And so that's going to be an area that I think the both criminally and civilly everyone's going to keep their eyes on is to what extent does the Supreme court, uh, potentially give a broad interpretation of CAFA. One that for example, the department of justice has been pushing that kind of really anyone that gets onto a computer without authorization [00:21:30] can be liable, or is it a more narrow interpretation that really, really is meant for hackers and only certain insiders and maybe not kind of everyone under the sun gets access to a, to a company's data.

Speaker 4: It sounds like you're trying to secure another spot on the, uh, performance review after that.

Speaker 3: Yeah. I wanna, I wanna be a repeat player on this one since it's so popular. So I want to get back if I can.

Speaker 2: So let's, um, let's talk a little bit about first of all. Yes, of course. I mean, you're going to have to get an extremely long line Todd, but [00:22:00] we should be able to screen you in. Um, but you, you, you had mentioned, uh, internal investigations, right? And that's when some of these things come to light and the employer first learns about this stuff. So if an employer is going through the files and uncover something that looks, you know, criminal, or, or, you know, touches on any of these things, there's a fraud issue. There's a trade secret issue. There's, there's something serious going on here. How should an employer go about doing that? Cause there's certainly a right way and a wrong way to conduct an internal investigation.

Speaker 3: [00:22:30] Well, first they're going to call us, uh, I know it was just getting, but it is true that what an employer wants to do when it does an investigation is ensure that the investigation is done with integrity. And so what you're gonna want to do is oftentimes at least consider whether or not you want to go outside of the company. Is there a concern about having HR involved? Is it going to create a potential conflict? The other aspect that you're going to want to consider is preserving information, [00:23:00] what steps need to be done to preserve any of the information that may be relevant to what you're looking at. Oftentimes you want to limit the amount of people that are aware of the investigation. And part of that is to preserve the integrity of it. The fewer people that know the less likelihood there is that people may start kind of getting rid of those documents, making the deletions Philip you mentioned.

Speaker 3: And so all of that really is geared towards [00:23:30] giving. Whoever's going to be conducting the investigation the best opportunity to really figure out what's going on. And then if you are working with counsel, whether it be in house, counselor, outside counsel, having them involved very early as well. If to the extent counsel is conducting an investigation, then potentially you're going to have the shield of the attorney client privilege and the work-product doctrine in place that may help with respect to, you know, going forward. How much of the information [00:24:00] becomes discoverable, civilly. All of those are different considerations that I think any time you want to make them almost immediately, when you learned that there's this potential for wrongdoing or potential of wrongdoing, because at the end of the day, what you're going to want to do is particularly if you're worried that there actually has been something that is going to put the company in harm's way criminally, you want to be able to be the one that goes to the department of justice, whoever the federal or [00:24:30] state law enforcement is and say, look, we, we learned about this.

Speaker 3: We've, you know, turned over every stone. We're coming to you to say, Hey, we want to work cooperatively to, to resolve it. And to the extent you haven't taken the steps upfront to preserve the evidence, uh, you haven't taken the steps to limit how many people know about it. It may make it much more challenging down the road to go to DOJ and say, you know, we've tried our best. If, if it turns out everything got deleted [00:25:00] because no one turned off the auto delete or everybody knew about it and started destroying documents, the department may not be all that happy with the investigation that was done internally.

Speaker 2: And is there a point you reached to, if you're an employer and you realize, okay, well, we don't think that the company is particularly in any real trouble here, but we've got an individual who certainly is what does a company do in, in that respect? I mean, when it comes to maybe contacting the department or taking whatever other steps might be appropriate,

Speaker 3: And this is another [00:25:30] classic situation where you have this criminal issue, but also a, an HR slash employment issue, the company is going to have to decide gleaning. If it's a director officer, does the company have an obligation to, for example, indemnify or at least pay for separate counsel for that director officer, to what extent to avoid a conflict? Because oftentimes, especially if you have a firm or in-house counsel

conducting the investigation, they're retained by the company, not [00:26:00] an individual. And so, you know, there could be privilege issues there. And also, you know, this leads to, uh, another situation where even if the company may not, at least initially believe that they, they face exposure, there could be situations of, you know, if it's a publicly traded company, they may have obligations to, to make certain public disclosures about wrongdoing within the company. And so there's, uh, a myriad of issues that arise that you kind of have to walk through about what do we do about [00:26:30] this other person? Do we wall them off? Does that have its own issues? Do we have to give them counsel, how do we navigate attorney client privilege in our discussions with this person? All of that, again has to, should be kind of considered upfront when you're beginning that investigation. So Todd,

Speaker 4: You mentioned war games. Now we're going to talk war stories, every guest who comes on the performance review, we have them give us some crazy employment story here. We're talking about the intersection between criminal activity [00:27:00] and employment. So do you have a crazy or a wild story for us?

Speaker 3: I, I unfortunately don't know how wild or crazy it is. I mean, I definitely have had a lot of prosecutions back in my former life, uh, that, you know, touched upon employment, definitely had, you know, securities fraud stuff where he had officers up to. No good are people at the hot end of the top of the pyramid is pilfering the company like, like crazy w one kind of, but I guess more apt to maybe some of the stuff we've been talking about today is that you can actually [00:27:30] have really low level folks who are engaged in criminal activity that that can cause some significant disruptions to accompany. And, and so, uh, one kind of string of cases I was involved with back when I was in, AOSA had to do with the DMV. And it's not an area you typically think about when it comes to federal prosecutions, but we actually did a whole series of these cases where he had fairly low-level DMV employees, many of which were kind of, you know, in a financial [00:28:00] strain who are willing to take bribes to give people licenses.

Speaker 3: And you know, it, wasn't kind of a one-off kind of situation. These would was a systematic effort by trucks, school owners to get commercial licenses for their students who couldn't pass the written or the driving test. And from the perspective of the department of justice, it was incredibly concerning because you had people who really weren't qualified to be operating big rigs, driving all over the [00:28:30] country with their California CDL that they paid five grand for. And so we ended up prosecuting for bribery because they were public officials, albeit kind of low level folks. And it kind of bringing back to what we talked about a little bit before we actually charged them with violations of Kapha, because none of these employees had the authorization to go into the records of the individuals to put in fake scores that they had passed the, you know, the written or the driving portion of the [00:29:00] exams, and then out shot a legitimate and at least not legitimate, but a real California driver's license.

Speaker 3: So they ended up getting charged with identity fraud as well. And so I think, you know, it's maybe not quite the crazy story that you guys have gotten from some of your colleagues, but, uh, I think it is a pretty good illustration that, you know, when you think about crime, including white collar crime and companies, you often think of the people

of the C suite or, you know, that kind of a situation and it [00:29:30] really can happen anywhere. And it, it also, I think is kind of illustrative that prosecutors have a pretty big toolbox to use when it comes to going after potential crime. And you just never know kind of how it's going to pop up and the consequences. And at least for some of the folks in those cases that I was involved with, they were talking multiple years in federal prison. And as a result of, you know, taking those bribes and issuing the licenses, all this, just [00:30:00] to drive a big rig, wow. It turns out you can make a fair amount of money as a, a long holler, at least for a little bit. So that, I guess was the incentive for the, for these folks. But yeah, it's a it's it was like I said, I don't have, it was a crazy case, but nonetheless one that, uh, was fairly shocking when it first came across our desks.

Speaker 2: Oh, it is, oh, I am a fat ugly agree with the department that it is concerning that people who failed the test or nevertheless being put on the roads. So I'm glad client department was [00:30:30] ahead of that one. Yeah. Yeah.

Speaker 4: Thank you for this story and, uh, for keeping our streets safe, but that brings us to the end of this episode to our listeners out there. Uh, we'd love to hear from you. Please email us at performancereview@gtlaw.com. And other than that, we'll catch you on the next one.

Speaker 1: [inaudible].