Original XpertHR podcast: April 25, 2017

Protecting Trade Secrets Before It's Too Late

David Weisenfeld: This is XpertHR.com – your “go-to” HR compliance resource for federal, state and municipal law. I’m David Weisenfeld for XpertHR.com, published by Reed Business Information and proudly partnered with LexisNexis.

On this podcast our focus turns to trade secrets issues. In this age of employees bringing smartphones and other electronic devices to work, the line between what's personal and what's work-related has become increasingly blurred. And that can make an employer's attempts to safeguard its confidential information dicier than ever.

So what can businesses do to prevent their valuable trade secrets from walking out the door with departing employees? And how much is too much when it comes to proprietary information?

For some answers we are now joined by California employment attorney, Dan Forman, who chairs the Unfair Competition and Trade Secret Practice Group at Carothers DiSante & Freudenberger in Los Angeles. Dan, it’s great to have you with us. [0:1:10.4]

Dan Forman: Great to be here, David.

David Weisenfeld: Dan, I'll start with this. The Federal Defend Trade Secrets Act of 2016 has attracted a great deal of attention because before it there was really just a patchwork of state laws. So what new remedies does the DTSA give to employers to protect themselves? [0:01:32.6]

Dan Forman: I’m glad you asked that. One interesting point is that that patchwork of state laws is still out there. The DTSA, unlike other federal laws, does not preempt existing state laws, so those various and sundry state Trade Secret Acts will remain in effect and will be enforceable.

In terms of what the DTSA brings to the table, that’s really new and innovative in this field, is the provision for an actual ex parte seizure of stolen trade secret property at the outset of litigation without any kind of service or notice to the defendant. This is something that will probably be used in very rare circumstances. There must be extraordinary circumstances demonstrated to the court, including showing a likelihood of success on the merits of the claim. There has to be a showing of immediate irreparable harm, such as the danger of destruction or the removal of the stolen trade secret materials if there is notice to the defendant.

Also what's interesting and innovative about this is, unlike traditional discovery, is the plaintiff or the party does not actually get the stuff. The seizure is taken down by law enforcement, and the court is to keep custody of material seized under the proceedings pending an initial hearing. So that's kind of interesting and it's certainly new, something to give lawyers a lot of chew on and a new tool in the arsenal against trade secret theft.

A couple of other things that are interesting that the DTSA brings to the table is that during the litigation there is almost automatic provision for stronger protection against trade secret information to the general public and that because we are now going to be able to prosecute these cases or defend these cases in federal courts under the DTSA, discovery, especially inter-state discovery, will be much easier for the parties to undertake. Currently under state law, taking depositions of people in other states is a much more difficult process whereas under the federal system it's a much simpler, much more straightforward process to get to the bottom of what went on.

David Weisenfeld: Dan, I mentioned at the top personal electronic devices. Does the Defend Trade Secrets Act address those, and what happens if an employee has been using his or her personal device for confidential work information? [0:04:05.0]

Dan Forman: Great question and it's a concern for all employers that goes to the underlying decision by employers as to whether they are going to allow a BYOD – a bring your own device – policy in their workplace.

The DTSA does not specifically deal with personal devices, but if an employer allows its employees to conduct confidential or trade secret work utilizing their personal devices or unsecured devices of any kind, it's going to hurt the claim down the road that the information was confidential and trade secret. It's going to hurt the employer's ability to claim that they took reasonable measures to protect their trade secret information.

So a BYOD policy, a bring your own device policy, still may be appropriate, but an employer really needs to make sure that they're taking adequate measures to secure their confidential trade secret information that might pass over those devices and that the employees agree at the outset that they'll allow those devices to be screened or wiped clean at the time of departure. The precaution is that those employees also agree not to share their devices with other people, their family members or other people who aren't employees bound by confidentiality.

David Weisenfeld: Now the DTSA has protections for employees as well, and one unique provision is that it provides immunity to whistleblowers who reveal a business's trade secrets to a government official or to his or her attorney about a suspected violation of the law. Dan, tell us about that one. [0:05:45.2]

Dan Forman: That's not really big news. It was part of the compromise that certain senators insisted be incorporated into the law. They were concerned that without that provision that the DTSA might be used to intimidate former employees who were bringing lawsuits, whether it was

whistleblower lawsuits or discrimination-type claim lawsuits. So like most other whistleblower protections or anti-retaliation protections in the employment sphere, this is not all that big news.

It does require, though, that if the whistleblower uses trade secret information in their litigation against their former employer, such as discrimination or retaliation litigation, that information, the trade secret information, must be filed under seal. So plaintiff attorneys are going to have to be very careful and diligent about how they use that information, because if they don't they may be asking for trouble when the defendants claim that they've violated the law by revealing trade secrets in conjunction with litigation.

The other aspect of this provision is that to get the full range of all damages that are available in the DTSA, employers must include the notice language about the whistleblower and non-retaliation provision in their confidentiality agreements or their handbooks or they may not be able to obtain the full range of damages that are allowed under the DTSA.

David Weisenfeld: Dan, even though this might not necessarily have been big news, I'd be remiss if I didn't ask in this age of WikiLeaks and the potential for increased whistleblowing in response to what's going on in Washington, about whether this could trickle down to the workplace with more employees claiming they need to use confidential information to blow the whistle on their employer. What are your thoughts about that? [0:07:36.4]

Dan Forman: I think whether there's an increase in whistleblowing claims and workplace employment claims depends largely on the economy and jobs. I think when you have a growing economy, overall there is less likelihood to whistleblow.

It will give employees who are operating under trade secret agreements probably a bit more comfort in being able to go to their lawyer and say, 'Here are confidential documents from my employer that I think are supportive of my whistleblowing case or that are in support of my job discrimination case.' But, it does not permit those employees to steal trade secrets. It simply says that you can show those to an attorney that's working for you or to a government official if you think something bad is happening.

Again, employee lawyers, plaintiff lawyers, are going to have to be very careful about what these employees bring to them and show to them. If the employees are simply taking the company's property that they think might help their case, information that may not be trade secret and fall under the Trade Secrets Act, those plaintiff lawyers, if they continue to hold on to that information, may be in violation of other laws, such as conversion.

If it's attorney/client information that comes from the company or the employer that is then showed to that lawyer, that lawyer will continue to have ethical obligations to not look at it and to turn it back to the employer or to their counsel and say, 'Hey, I seem to have gotten some inadvertently produced attorney/client privilege or work product materials, and I can't use them and you need to have them back.' So

that's going to create potential claims against both former employees and their lawyers relating to those ethical issues.

In California we have some very good case law that says that employees can't do this type of activity and that they can't resort to self-help to support their cases, they have to go through discovery to obtain documents that may support their case, as opposed to stealing things from their employer and giving them to their lawyer to uphold their claims.

David Weisenfeld: Self-help is a nice way of putting it, but I take it you mean by that not simply just taking something off the computer and bringing it to their lawyer? [0:10:01.2]

Dan Forman: That is one type of action, that is self-help or theft. What I think this provision does in the DTSA it says that if you're in a DTSA case in federal court, an employee can't do that with respect to trade secret information without running afoul of the DTSA. It doesn't say that you can simply take whatever you want and show it to your lawyers because you think it supports your employment claim or your retaliation claim.

David Weisenfeld: Again, we're speaking with California employment attorney Dan Forman, of Carothers DiSante & Freudenberger in Los Angeles. Dan, with trade secrets issues generally, is there a best strategy for employers to address these potential issues at the hiring stage before problems arise? [0:10:48.7]

Dan Forman: In fact, David, I think you need to, as an employer, address these issues even before hiring. A strategy that employers should consider is utilizing confidentiality agreements as part of the interview process. An agreement whereby applicants not only agree that they're going to keep anything that they learn during their interview process about that employer as confidential, but also to advise them and have the applicants confirm or warrant that they are not going to reveal any of their current employer's confidential information.

So as an employer you are creating a shield against a claim down the road that applicants came over and gave you, the new employer, confidential or trade secret information that they weren't supposed to.

Employers will want to update their confidentiality agreements, their handbooks, with the whistleblower anti-retaliation notice provisions to make sure that they are availing themselves of the full range of potential remedies down the road. It's always good to maintain vigilance. If an employer has a lot of confidential and/or trade secret materials that they are concerned about, background checks are another way of looking into someone. Reference checks, checking on their prior employments, whether they've been successful and long-lived or very short-lived and problematic.

Many of these cases unfortunately seem to involve employees who are long-term employees, who are trusted employees for a long time who then, if something happens, they make a decision. They're upset, and they decide they're going to go and move their business to a new place of employment or start their own competing business and then they take trade secrets and confidential information with

them to shortcut that process. So it's hard to protect against that kind of incident just in the hiring process alone.

David Weisenfeld: With that said, though, is there anything specific, as someone who counsels employers in this area, that you like to see policies including to safeguard the information? [0:12:58.0]

Dan Forman: Absolutely. Employers should definitely use their counsel to adopt appropriate policies for their business. Among other things, they need to consider precluding and should preclude employees from using trade secret or confidential information from former employers absent written consent.

An employer should be identifying in their policy with as much specificity as possible the types of materials they consider to be confidential and trade secret. Certainly identifying every single piece of paper ever created or touched in an office setting is probably not something that will hold water down the road, so there should be some attention to specificity as to why and what is designated as trade secret. That can be done in conjunction with both agreements, handbooks, as well as actual training of employees, retraining of employees on both confidentiality and protocols to use when working with confidential materials - checking them out, checking them in, tracking them, that kind of thing.

Also, it's very good to have a computer usage policy whereby employees acknowledge that what they do on an employer's computers or computer systems, including on the internet while accessing it through the employers, are within the employer's proprietary realm. If they're accessing the internet to do something personal it's not their right to privacy. They need to know that by using the employer's computer systems that they have no right of privacy in what they do, even if it's for themselves.

What's also very helpful is to have employees agree at the time of hiring and periodically that what they create at work or on employer property or during work is the employer's property. It's proprietary to the employer. It's not to be shared outside of the work setting and must be returned, and they agree to return it at separation.

These things need to be reviewed periodically. Password changes are highly recommended. Security protocols are needed. Depending on the type of business there may be differing levels of confidentiality and confidential information, and those things should be dealt with appropriately so that only people with a need to know get access to it and take reasonable steps to maintain its confidentiality.

And it's not really a policy, but employers can work with their IT experts to set up ways to monitor and to alert them about unusual activity on their systems, whether it's offloading information onto a flash stick, downloading materials onto the cloud, through email or even the old-fashioned way of printing out a large amount of information. There's ways that the IT security people can trigger alerts and alarms that either stop that kind of activity or alert somebody to that type of activity, so that it can be shut down and/or further monitored.

David Weisenfeld: Dan, it's important to note that not all trade secrets are necessarily all that secret, the Colorado Court of Appeal recently threw out a verdict in a misappropriation of trade secrets case – *Hawg Tools v Newsco* – because it found the information at issue wasn't truly secret. So with that said, can employers overreach in trying to protect too much? [0:16:33.2]

Dan Forman: They can. That wasn't really the issue though. The overprotection wasn't really the issue in that case. But yes, as I mentioned, in the policies you want to have some kind of specificity as to what you are calling confidential and how you treat it to make sure that you maintain it in a confidential area.

In the *Hawg* case, what was interesting was that the employer hired a designer to create a unique part under a confidentiality agreement, and the designer created that part and then went to work for a competitor and designed a very similar part. So the Hawg Tools company sued the competitor and the designer for trade secret misappropriation and the designer for breach of contract.

In that case the court analyzed the expert witness testimony and concluded that Hawg and the defendant's parts were identical and that Hawg had made reasonable efforts to maintain secrecy, but because there were (according to the expert witness testimony) other, essentially identical designs, that were in the public domain – you could go down to the library and find a design to make that part, which is not a secret – because of that while Hawg had maintained its design in confidence, it did not have trade secret value. Because to be a trade secret, an employer has to keep the information confidential and that information has to have value to that employer because it is confidential, and it is not publically available in another format or form.

And what I thought was really interesting was that the court, in reaching its conclusion and reversing the jury verdict that there had been misappropriation of a trade secret on this sort of expert basis, also concluded that Hawg could maintain the breach of confidentiality contract agreement against the designer, who then went on and worked for the competitor.

So it's an interesting case and there's a lesson in it, which is that if you're going to pursue something as a trade secret, it really can't be available by another means, by Google or by going down to the library and finding the equivalent information out there in the public domain.

David Weisenfeld: Good point. Well we only have about a minute or so left, so Dan do you have a final piece of advice that you'd like to share with employers? [0:19:00.1]

Dan Forman: At separation it's so important to turn off any employee's remote access, to change passwords that employees may have had access to, and to take affirmative action to ask and ensure that those employees who separate return any company property and certainly return confidential and trade secret information that they may have had, especially if they had a personal device or that they may have

had in their home office or in their briefcase or wherever. It's just important to make those efforts so that down the road nobody claims, 'Hey, you didn't make any reasonable efforts to protect your confidential information.'

David Weisenfeld: Dan Forman chairs the Unfair Competition and Trade Secret Practice Group at Carothers DiSante & Freudenberger in Los Angeles. Dan, thanks so much for joining us and sharing your insights. [0:19:52.1]

Dan Forman: Thanks, David, and I can be reached at dforman@cdflaborlaw.com.

David Weisenfeld: I'm David Weisenfeld. We hope you've enjoyed this podcast, and for more on this topic, you can check out XpertHR.com's How to Protect Information under the Defend Trade Secrets Act. Continue checking our website regularly for more podcasts on key employment-related issues, including "Making the Most of Mobile Recruiting."

The opinions expressed in this program do not represent legal advice, nor should they necessarily be taken as the views of XpertHR or its employees. XpertHR.com is published by Reed Business Information, and is proudly partnered with LexisNexis.

For more information about XpertHR, our subscription offering, or our 50-state Employee Handbook, call us toll free at 1-855-973-7847. Again, that's 1-855-973-7847.