BY COURTNEY MCGEE
Anderson Zeigler

THE (TRADE) SECRETS TO SUCCESS:
How To Protect Your Information In A Competitive Marketplace

More often than not, the employees that leave your employ for a rival business are the ones who hold the (trade) secrets to success. Their know-how makes them a desirable candidate across the industry.

But often times, this know-how is not theirs to take, and disclosure of this profitable and confidential information amounts to a data breach, as well as an issue of trade secret misappropriation.

Sixty percent of data breaches were caused by unauthorized or malicious use of company resources by employees or trusted insiders — states Verizon's 2017 Data Breach Investigations Report — and 15% of those breaches involved an employee or insider taking data to start a competing company or to work for a competing employer.

The issue of data theft and trade secret misappropriation by current and former employees is not new, but it is intensifying. Indeed, the dissemination of information is getting easier and easier; everything is digital and everyone is connected, making the taking and disclosing of a company's trade secrets effortless, and often unnoticeable. Plus, once commingled with a rivaling company's own information, the former employee's or rival's misuse may not be easily prevented — or even remedied.

"It [would] be a bone crushing endeavor", said the Northern District Court of California, when considering whether it could identify and enjoin the use of Waymo's trade secrets, which were found to have been wrongfully provided to rival Uber by a former Waymo employee. "And, even then, it may prove impossible to fully restore the parties to their respective competitive positions as if no misappropriation had occurred. It is far better to instead put in prophylactic measures now to prevent misappropriation."

So what "prophylactic measures" should businesses take to prevent private information from falling into the hands of a competitor? Unfortunately, the evolving nature of technology and the workplace, paired with unestablished and unclear intellectual property and competition laws, do not lend a definitive answer.

What if a business requires employees to sign non-compete agreements, restricting their employment with competitors upon separation from the business? Unlikely. In California, non-compete agreements are generally unenforceable; the State's policy rejects restraints in trade, encouraging employee mobility instead.

How about if the business invokes another state's laws to govern the non-compete; for example, if the business has nationwide locations or employees in varying states? It is unclear. While it may seem wise to have the law of a state that allows non-competes govern your agreement, California case law is inconsistent in upholding choice of law provisions in that context.

Can the business stop the former employee from working with a rival after hired, if it is clear that trade secrets will be used in the new employment relationship? Again, it depends. Many states allow former employers to bring an action to enjoin a former employee from employment with a competitor in circumstances when it is presumed the employee will rely on the former employer's trade secrets due to the similar nature of the jobs. Of course, the trend amongst California case law is to reject this inevitable disclosure doctrine (surprise!). California courts have held that "the inevitable disclosure of trade secrets doctrine transforms employee access to trade secrets into a de facto non-competition agreement."

Thus one thing is clear- attempting to remove the risk of the employee working in a similar but competing position is not the answer.

So what should a business do? To start, it can focus on the concept of secrecy.

The very definition of "trade secret", of course, requires secrecy. California law provides that, for information to be a "trade secret", it must both (1) "derive independent economic value … from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use" and (2) be "the subject of efforts that are reasonable under the circumstances *to maintain its secrecy*." In other words, if a business fails to take precautions in regard to its information, the above-discussed strategies for dealing with departing employees would not work anyway, as the business would first have to prove it tried, using commercially reasonable efforts, to prevent the theft or misuse of the information.

Accordingly, to determine the best way to maintain secrecy, I find it helpful to look to a survey of California cases that discuss which precautions, when taken, are probative of the existence of trade secrets.

Those precautions include:

• ***Advising employees of the existence of trade secrets and the importance of confidentiality.***

This should include having — and using — a written policy regarding trade secrets, as well as training in connection with the policy. Even employees who are not necessarily provided access to the trade secrets, and have no knowledge of what the trade secrets consist of, should be involved, as they may still be in charge of security measures and protocols around the workplace. In addition, it is a good practice to have a point person, either internally or externally, that you can rely on in response to data theft. Remember that many times such theft affects more than just the interests of the employer-business. Where private client or customer information is taken, the law may require certain procedures be followed, including notice to those individuals and certain regulatory agencies.

• ***Limiting access to trade secrets on a need to know basis.***

This means that only employees who need to know trade secrets in order to perform their job duties, should be granted access to them. In addition, those employees (as well as any suppliers, contractors and even clients, if appropriate) with access, should sign confidentiality or nondisclosure agreements, which clearly explain what information might be the subject of their confidentiality obligations and what safeguards and precautions they must take consistent with those obligations.

• ***Actually enforcing or policing access to trade secrets.***

This should include the use of passwords or encryption on confidential information, and the requirement that such measures be used on company, or especially, personal devices. This should also include a requirement that employees promptly return those passwords — or any equipment or information in their possession containing confidential information — upon their separation from employment.

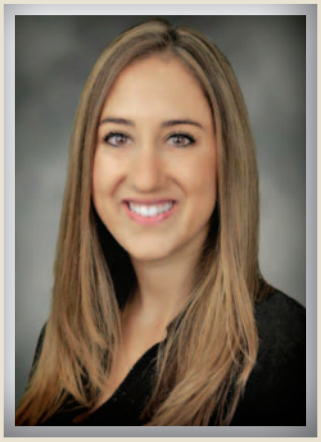
In addition, attentiveness, modification and innovation are always important. Many businesses stay loyal to the routines they are used to and have traditionally maintained. While this is beneficial in some respects, they should also take care to adapt to changing laws and tech, and reassess their policies and protocols as needed. At my firm, there are a few employees with rolodexes on their desks that I marvel at! But the fact of the matter is that employees are not generally going to be departing employment with rolodex in hand; rather, the worry is that employees will be transferring client and customer lists via email, USB device or other electronic means that allow for easy copying and distributing.

Why, you ask, should a business take all of these precautions if it may not be able to prevent the employee's move to a rival company anyways? Because if it comes to that, at least you have the fundamentals needed to challenge any potential collusion and bring a successful action for misappropriation in the future. Though you cannot restrict competition, you can — and must — still take steps towards the protection of your competitive assets. ■

About the author...

Courtney McGee

Courtney McGee's practice is focused primarily on business, intellectual property and employment matters. She assists individuals and businesses with employment and labor law issues, negotiating and completing commercial transactions, and utilizing and protecting intellectual property and other proprietary information. As a Sonoma County native, Courtney appreciates having the opportunity to represent and work with local businesses here in Wine Country.



ANDERSON ZEIGLER
ATTORNEYS AT LAW A PROFESSIONAL CORPORATION

50 Old Courthouse Square
Santa Rosa, CA
707-545-4910
www.andersonzeigler.com