FIVE STEPS TO PROTECT YOUR TRADE SECRETS WITHOUT A NON-COMPETE

AMELIA L. B. SARGENT is a partner with Willenken LLP, in Los Angeles. Her practice focuses on trial and appellate litigation for clients in a wide range of industries—from electric car start-ups, to established biopharmaceutical companies, to mobile game developers—with a particular focus on intellectual property and trade secret disputes.

She was also the driving force in forming Willenken's art, cultural, and educational institutions industry group, which provides representation and counseling in a wide range of matters. She teaches Art and the Law at the University of California, Hastings College of Law. Through regular contributions to the American Bar Association Section of International Law: Art & Cultural Heritage Law Committee's quarterly newsletter, publications in academic journals, and presentations at industry conferences such as ALI CLE's Legal Issues in Museum Administration, Amelia also shares her specialized knowledge of this area with the wider legal community.

How do you protect your trade secrets? If the answer is by imposing non-compete clauses on your workforce, there's bad news: As trends in trade secrets go, non-competes are on their way out.

Relying on non-compete clauses in contracts has historically been a very common and relatively easy way for a business to protect trade secrets and confidential information. By restricting departing employees from taking new positions in the same industry, employers hope their confidential and proprietary business information can be protected from their competitors. For many companies, imposing—and enforcing—a non-compete that restricts the worker is much easier than identifying any particular "secret" to protect. Indeed, that is what makes trade secret law so interesting. While other types of IP are defined by what *they are*—an invention, a writing, or a logo or design—trade secrets are largely defined by what *you do*. Do you keep it secret and is it valuable because it is secret?

But the use of blanket non-competes to protect business information is quickly becoming disfavored as policies protecting worker mobility rights gain steam. On July 9, 2021, President Biden signed an executive order to promote competition in the economy.[1] Among other policy statements, the order identified non-compete agreements as a cause of a worsening imbalance between "[p]owerful companies," restricting workers' ability to change jobs and "making it harder for workers to bargain for higher wages and better work conditions."[2] The order encourages the Federal Trade Commission to exercise its rulemaking authority "to curtail the unfair use of non-compete clauses and other clauses or agreements that may unfairly limit worker mobility."[3] The White House hopes limiting these clauses will stimulate economic mobility by increasing competition and wages, and allow workers to change jobs more easily.[4]

At the national level, this trend continues a policy goal of the Obama administration which issued a "call to action" encouraging state legislatures to ban or narrow the use of non-competes.[5] Indeed, since 2016, more than a dozen states and the District of Columbia changed their non-compete laws to provide more protections for workers.[6]

As non-compete clauses fall out of favor, California practice can serve as a model for how to protect trade secrets. Non-competes have been generally unenforceable in California for more than a decade, after the California Supreme Court held definitively in *Edwards v. Arthur Andersen LLP* that non-compete agreements are invalid unless expressly permitted by statute.[7] In California, public policy favoring

employee mobility is codified in Business & Professions Code section 16600, which provides that "every contract by which anyone is restrained from engaging in a lawful profession, trade, or business of any kind is to that extent void."[8] Thus, in California, laws protecting trade secrets must always be balanced against the rights of employees to change jobs and the rights of employers to freely hire valuable talent.

The policy shift supporting employee mobility and economic competition is, of course, not the only reason to reassess trade secrets now. The rise of remote work poses a special threat to trade secrets, both from employee activity (deliberate or accidental) and outside threats such as hacking, phishing, or spoofing. The sudden shift to remote work during the COVID-19 pandemic meant employees began using personal devices, such as home computers, laptops, or flash drives, and personal wi-fi connections to perform their work. Unable to access secure offices, employees began working at kitchen tables, with kids, spouses, or roommates nearby. HR activities such as furloughs and layoffs—and now hiring and onboarding—may have been conducted remotely, or in a rushed manner.

The apparent waning of the pandemic does not appear to spell the end of remote work: Many companies have not yet required employees to return, and some are adopting hybrid schedules or even going fully remote. A PricewaterhouseCoopers survey reported that over half of white-collar employees want to continue working remotely three days a week or more, even after the pandemic ends.[9] Now that the pandemic is in its second year, courts will expect companies to have appropriate measures in place to protect their trade secrets—upgrading their technology and HR policies in keeping with remote work's "new normal."

Protecting a company's trade secrets without infringing on employee mobility requires the cooperation of management, HR, and IT, with legal leading the way. For those of you who rely on non-competes, or just need to tune up your trade secret know-how, here are five steps to protect a trade secret *without* a non-compete:

STEP 1: IDENTIFY YOUR BUSINESS'S TRADE SECRETS

A trade secret is defined by the federal Defend Trade Secrets Act (DTSA) as information that: (i) "the owner thereof has taken reasonable measures to keep … secret"; and that (ii) "derives independent economic value, actual or potential, from not being generally known" by a person who could use it.[10] This definition tracks the Uniform Trade Secrets Act (UTSA), which all states except New York have adopted in some form. Classic examples of trade secrets include the formula for Coca-Cola and the recipe for Kentucky Fried Chicken. But a trade secret can be any kind of information, as long as it meets those two criteria.

Trade secrets can include business and marketing plans, budgets and financial projections, software processes and applications, compilations of data, pricing and vendor information, product specifications, prototypes, and processes. Even negative information—how *not* to do something—can be a trade secret. Trade secrets do not even need to be written down.[11] This makes it tempting for businesses to declare that all of their information falls within the definition of trade secrets.

But the first step to protecting a trade secret effectively is knowing what it is. In fact, California requires litigants to identify the trade secret "with reasonable particularity" before allowing discovery to begin.[12] Some federal courts have adopted a similar requirement,[13] and the Sedona Conference's Working Group on Trade Secrets has released a Commentary supporting identifying trade secrets up front in litigation.[14] A poorly defined trade secret can render plaintiffs vulnerable to defensive tactics that can add significant cost and delay to litigation.

Instead of waiting for litigation, IP lawyers should sit down with the business side to understand what really makes their business tick to save a lot of energy (and money and heartache) when protecting trade secrets. Narrow and easily defined trade

secrets are much easier to protect. The fact is, many of the trade secrets that a business might have are not that valuable or have a very short shelf life—only a few months before a product is released, a patent is obtained, or a marketing initiative goes public. A business considering litigation, or a major IT upgrade, or other expenditure may find the value of its trade secrets does not justify the cost. But when identifying a trade secret, be sure not to go just to the core business, but also to marketing, strategy, sales, and other departments. Every department can have protectable information that might constitute a trade secret.

STEP 2: EDUCATE MANAGEMENT AND YOUR EMPLOYEES ABOUT WHY TRADE SECRETS MATTER

Use Step 1 as an opportunity to partner with the business side to create a culture of awareness around trade secrets. Happily employed workers usually want to do the right thing—help the company grow and succeed. Protecting trade secrets is part of that process. Don't let the fine print of the employee handbook be the only explanation a valuable employee receives about what the company considers confidential, proprietary, and trade secrets. Instead, design a training session to educate employees about what trade secrets they may be handling and how to protect them. Be sure this training includes trade secret basics, such as marking documents as confidential and not emailing documents outside the company, as well as clear explanations that such information belongs to the company, not the employee.

Engage management in encouraging (and modeling) good trade secret habits and clearly communicating to employees what information the company regards as trade secrets, especially because the company's trade secrets change over time. This helps employees make good choices to protect trade secrets from accidental disclosure. (Imagine your sales rep sitting at the bar after a long day at an industry conference, gossiping about your upcoming plans with the sales rep from your competitor!) If employees know that certain information is sensitive, they are less likely to disclose key details that could damage the business at critical times.

STEP 3: TUNE UP YOUR HR POLICIES AND PROCEDURES

You may have to blue-pencil that non-compete, but HR policies and procedures are still the gold standard for protecting trade secrets. The employee handbook, confidentiality and invention assignment agreements, and NDAs are still valid and enforceable contracts (and the DTSA and UTSA never preempt breach of contract actions). Just remember, overbroad confidentiality provisions that seem to be non-competes in disguise will be disfavored by courts.[15]

When onboarding new employees, make sure HR explicitly addresses trade secrets and confidential information, and require a signed acknowledgement of the employee handbook. (If you're remote, require a DocuSign or Adobe E-signature.) Ensure the employee signs an NDA or privacy waiver, if need be, and have them certify that they are not bringing confidential information from any previous employer, especially any competitor. Be sure any equipment provided is recorded and logged by HR or IT.

When offboarding, do it all again in reverse: Require and log the return of equipment immediately, and shut off email and access to sensitive company information. Remind departing employees of their continuing confidentiality obligations. Have the departing employee sign an acknowledgement of this reminder, and certify that they are not taking any confidential information with them.

STEP 4: INVOLVE THE IT DEPARTMENT TO IMPLEMENT YOUR SECURITY—ESPECIALLY WHEN REMOTE WORK IS INVOLVED

Use technology to its fullest to protect trade secrets. How do the teams in your business communicate and send information?

Available tools include cloud-based services, remote desktops and VPNs, videoconferencing, chat platforms, paperless capabilities, and monitoring software. IT can restrict access to files or folder

structures by department, group, or even by person to make sure sensitive files are accessible only by those who "need to know." Similarly, individual documents can be branded as confidential, and restricted with passwords or read-only rights to prevent printing and copying.

For companies with very sensitive trade secrets, monitoring software can be implemented to watch for unusual downloading patterns or deletion activity, or to track individual documents. Activity logs are often available to track access to cloud-based documents and can be reviewed on a regular basis for unusual patterns.

You'll want to assess whether particular tools raise legal or privacy concerns that are specific to your jurisdiction. But once you've identified your trade secrets and created a culture of awareness among your employees, IT tools can be fine-tuned to balance privacy concerns with protections that the company needs.

STEP 5: WATCH OUT FOR EMPLOYEES MOVING BETWEEN COMPETITORS

In a world without non-competes, employees can change companies easily and businesses can freely hire valuable talent from their competitors. But companies on either side of the deal should consider extra precautions to protect their trade secrets, and to protect against inadvertently receiving trade secrets from others.

Employee going to a direct competitor

A situation like this may require more than the ordinary offboarding but it is much easier to deal with if you have laid the groundwork to create a culture of trade secret awareness. The employee should be reminded of their obligations to keep company information confidential. This reminder can be backed up by utilizing the monitoring and anti-deletion tools mentioned above, to confirm whether there has been any unusual access or computer activity. Companies with particularly sensitive trade secrets may want to consider whether to cut short the notice period to effect the termination immediately. And before a worker's computer or laptop is issued to someone else, an employer may want to consider preserving a forensic copy to ensure that confidential information was not taken.

If a company believes trade secrets may have been taken, it should take immediate steps to preserve all electronic data and hardware and consider engaging outside counsel right away. A full forensic investigation often requires the use of an outside vendor, but can yield critical evidence. In addition, it may be appropriate to send demand letters both to the former employee and the new employer notifying them of the potential claims. Acting quickly is critical for both protecting the trade secret against use or disclosure, and as later evidence demonstrating reasonable efforts to protect the trade secret.

Hiring from a direct competitor

Just as important as protecting its own trade secrets, a company hiring from a direct competitor needs to protect against inadvertently receiving misappropriated trade secrets from others. Again, creating a culture of trade secret awareness is key in sending new employees a clear message that the wrongful use of information from prior employers will not be tolerated. Companies should reinforce this message at hiring, during onboarding, and within the new employee's team. During onboarding, companies should consider having employees certify that they have not brought any information from their former employer.

If a company receives a demand letter alleging that a new hire has misappropriated trade secrets, it should immediately preserve all electronic data and hardware, and send out a litigation hold. Consider engaging outside counsel early, as there are many pre-litigation pitfalls. For example, you may want to conduct a forensic investigation, but deleting or altering any electronic data—or even looking at it—risks altering key evidence that could be used to defend the case. A company's response to a demand letter will likely determine whether it can avoid litigation.

CONCLUSION

Employees moving to and from competitors will be an inevitable scenario as non-compete agreements become less common. Don't wait for litigation to figure out what your trade secrets are and how to protect them. Using these five steps as a guide, companies can start to proactively manage their trade secrets to keep them protected in a fast-changing world.

Notes

1 Executive Order on Promoting Competition in the American Economy, July 9, 2021, available at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/.

2 Id.

3 Id.

4 Fact Sheet: Executive Order on Promoting Competition in the American Economy, July 9, 2021, available at https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/09/fact-sheet-executive-order-on-promoting-competition-in-the-american-economy/.

5 State Call to Action on Non-Compete Agreements, available at https://obamawhitehouse.archives.gov/sites/default/files/competition/noncompetes-calltoaction-final.pdf.

6 Charles Guzak, Lawrence Lorber, Scott Mallery, and Leon Rodriguez, Policy Matters Newsletter, July 2021, https://www.jdsupra.com/legalnews/policy-matters-newsletter-july-2021-2528539/.

7 Edwards v. Arthur Andersen LLP, 44 Cal. 4th 937 (2008).

8 Cal. Bus. & Prof. Code § 16600.

9 It's time to reimagine where and how work will get done, PwC's US Remote Work Survey, Jan. 12, 2021, https://www.pwc.com/us/en/library/covid-19/us-remote-work-survey.html.

10 18 U.S.C. § 1839(3).

11 See, e.g., Greenly v. Cooper, 77 Cal. App. 3d 382, 392 (1978).

12 Cal. Code Civ. Proc. § 2019.210.

13 See, e.g., InteliClear LLC v. ETC Global Holdings, 978 F.3d 653, 658 (9th Cir. 2020); IDX Systems Corp. v. Epic Systems Corp., 285 F.3d 581, 583 (7th Cir. 2002).

14 The Sedona Conference, Commentary on the Proper Identification of Asserted Trade Secrets in Misappropriation Cases (Oct. 29, 2020), available at https://thesedonaconference.org/node/9717.

15 See Brown v. TGS Management Co, LLC, 57 Cal. App. 5th 303 (2020).