September 01, 2020

When the Levee Breaks: Preparing for a Flood of Trade Secret Litigation

It's no exaggeration to say that the COVID-19 crisis also could be the trade secret crisis of a generation.

By Chris Patton

We are monitoring the coronavirus (COVID-19) situation as it relates to law and litigation. Find more resources and articles on <u>our COVID-19 portal</u>. For the duration of the crisis, all coronavirus-related articles are outside our paywall and available to all readers.

Maybe you're old enough to remember the action movie *Ronin*? Robert De Niro plays the trope of the lone mercenary reluctantly taking "one last job" before he retires. At one point, a brooding De Niro reflects on all of the spooks and bruisers who flooded his rarified trade after the Cold War ended: a glut of talent on the dirty secrets market. Pure Hollywood, right?

Not entirely! The tricks of any trade can have commercial value. When spy rings and sports teams fall on hard times, laid-off employees can walk out the door with trade secrets in tow. And with this COVID-19 train wreck still grinding down the track, corporations are getting jittery about ex-employees sharing trade secrets with their new employers in the general job-search melee. As unintentionally leaky work-from-home spaces become the new normal, it's no exaggeration to say that the COVID-19 crisis also could be the trade secret crisis of a generation.

Trade Secrets: Overview

Trade secrets are often said to be the murkiest area of intellectual property law. Patents define inventions; trademarks stake out brands. But what qualifies as a trade secret?

In 49 states, trade secrets are defined under some version of the 1985 Uniform Trade Secrets Act (UTSA). The UTSA ticks off a long list of business practices and information that derive commercial value from the fact that they aren't generally known or easily obtained, and for which their holders have made "reasonable efforts," under the circumstances, to protect their secrecy. Unif. Trade Secrets Act § 1 (amended 1985), 14 U.L.A. 538 (2005).

^{© 2020} by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

In 2016, Congress passed the Defend Trade Secrets Act (DTSA). This newly created federal cause of action mostly follows the UTSA's *trade secret* definition. 18 U.S.C. § 1836 *et seq*. Although substantively similar to state law counterparts, the DTSA has proven to be a particular boon to plaintiffs in trade secret cases. In fact, one analysis found that since the DTSA's passage, trade secret litigation in federal court has increased by nearly 25 percent, while the same period saw other types of intellectual property cases either remain constant (patent) or slightly decline (copyright and trademark).

Common Types of Stolen Secrets

While some high-profile corporate espionage capers—such as the 2009 China-based hack on Google—make for good reading, in most cases the misappropriated trade secret is something fairly mundane: a customer list, pricing and cost information, a marketing strategy, or customer account information. And most trade secret lawsuits spring from some type of commercial business relationship, such as an employee who leaves one company to join a competitor, or a vendor who obtains a company's trade secret information as part of an ongoing relationship.

The Rising Tide of Trade Secret Lawsuits

The number of trade secret cases in the United States has steadily increased since 2008, when the Great Recession upended markets. This growth is likely due to several factors, including higher employee turnover, increased use of outside contractors, more workfrom-home flexibility, the reduced ability of employers in some states to enforce noncompetes, and the passage of the DTSA.

While these factors still apply today, the current pandemic creates even thornier problems for companies trying to keep trade secrets out of their competitors' hands. Indeed, as many employers try to keep afloat in the wake of constantly evolving stay-at-home orders, a virtual office can become a virtual sieve. This unplanned diffusion of trade secret information to homebound employees becomes even more problematic when those employees have to be laid off or furloughed. And for former employees eager to gain a leg up with their new bosses, easy access to their previous employer's trade secrets can offer a tempting advantage.

Preparing for the Coming Surge

In these challenging times, many employers ask what they can do to ensure that "reasonable efforts" are taken to maintain the secrecy of valuable information. Assuming that most employers have already required their employees to sign a confidentiality agreement during the hiring process, the first—and the easiest—step is to simply remind

^{© 2020} by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

Corporate Counsel Summer 2020, Vol. 34 No. 3

those employees that they must still keep company information confidential even when working from home. Other simple steps include strictly limiting trade secret access to those employees who need it to carry out their job responsibilities. And keeping trade secret information in a password-protected database can deter casual or unintentional sharing.

When home-based employees have to be let go, it is even more important to take steps to ensure that trade secrets are safe. Employers must be proactive in reminding departing employees of the ongoing nature of any pretermination confidentiality obligations. It is also essential to make sure that departing employees return any confidential hard-copy or electronic information they have been using. This includes confirming that departing employees are not carrying confidential information on their personal devices, including phones, home computers, and even USB or thumb drives (so often discovered, months later, adrift at the bottom of desk drawers).

Of course, what constitutes "reasonable" protection depends upon the specific circumstances. Regardless of the situation, though, the upheaval following the COVID-19 crisis should spur companies to take a hard look at old playbooks and to prepare for a "new normal" in trade secret protection and defense. For corporations hoping to ride out the COVID-19 flood—and the wave of trade secret litigation that COVID-19 is likely to unleash—such a reassessment isn't just prudent. It's essential.

Chris Patton is a partner at Lynn Pinker Hurst & Schwegmann, LLP in Dallas, Texas.

^{© 2020} by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.