Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

How To Keep Trade Secrets Safe

By **Braden Campbell**

Law360, New York (November 23, 2016, 12:35 PM EST) -- In his 25-year career as its public face and de facto chief executive, celebrity chef Christopher Kimball helped build America's Test Kitchen into a culinary empire spanning television, print and the web. Then, he stabbed his former company in the back, according to a lawsuit filed last month in Massachusetts state court.

In its suit, America's Test Kitchen accuses Kimball of stealing its proprietary media contacts, business practices and copyrighted recipes and poaching several employees for his new venture, Milk Street, which it says "literally and conceptually ripped off America's Test Kitchen."

That America's Test Kitchen allegedly fell victim to trade secrets theft at the hands of its former star is a reminder that any company is vulnerable to losing such intellectual property. Here, attorneys provide tips on how companies in any industry can keep their trade secrets safe and stem the bleeding if the secrets get out.

Trade Secrets Aren't Just for Tech Firms

To a public whose popular image of trade secrets theft is a black-clad thief descending "Mission: Impossible" style into a Silicon Valley vault, cake recipes hardly sound like something to file suit over. But for companies in today's crowded marketplace, most pieces of privileged information that give them an edge over competitors can be a trade secret.

"It's a popular misconception that trade secrets usually apply to high-tech companies," Fisher Phillips employee defection and trade secrets practice co-chair Bob Yonowitz said. "In theory, every business can have trade secrets. If you have competitive data you've developed that gives you advantages in the marketplace that other companies aren't aware of, you have potential trade secrets."

Indeed, any company in any industry can have a trade secret. Attorneys will often cite Coca-Cola's formula and Kentucky Fried Chicken's "11 herbs and spices" as trade secrets, but something as simple as the way a home goods chain arranges its wares can qualify if there's privileged knowledge behind it.

"How do we go about decorating our windows?" Morgan Lewis & Bockius LLP trade secrets litigator Larry Turner asked. "Do we have a study, for example, or position on the colors that we use? Do we have a particular time of day that we believe is more advantageous for the customer to come to us for products or services?"

Of course, not everything is a trade secret. To qualify for protection, such knowledge must genuinely not be known by competition, and it has to involve a unique process or methodology. But even if those boxes are checked, a trade secret won't necessarily merit protection in a court's eyes unless its owner takes certain steps.

Implement Protective Policies

The first step toward protecting a trade secret, attorneys say, is treating it like it's valuable. If a company has to go to court to protect its secrets but hasn't taken clear steps to protect it, judges won't be very sympathetic.

"You have to be able to demonstrate reasonable efforts to maintain its secrecy," Yonowitz said. "The court isn't going to treat it like a diamond if you don't treat it like a diamond."

There are several ways employers can go about treating their trade secrets like the precious gems they are. Yonowitz recommends to clients that they meet with workers to lay out, explicitly, what aspects of their business they consider trade secrets. And it may sound cheesy, but if a secret is written down, it needs a mark designating it as confidential, he said.

Once a company has made clear what it considers to be its trade secrets, there are several policies it can implement to protect them. Confidentiality agreements are a no-brainer, but companies should also have their employees sign an agreement explaining employees have no expectation of privacy on company devices. Other recommended measures include keeping trade secrets under password protection, limiting access to only those who need it to do their jobs and blocking workers from using their personal devices for company business, if possible.

With almost all information now stored digitally rather than physically, the only tool needed to steal it is a thumb drive. As such, one of the most important protective measures a company can take is to implement software that tracks how employees access company technology and to maintain a team that knows what to watch out for.

"Almost all of it, 98.9 percent of trade secret theft, occurs using computer technology and computers," Paul Hastings LLP international employee mobility and trade secrets practice head Bradford Newman said. "Gone are the days where you lug a box full of documents out."

But it is possible for companies to go overboard in protecting secrets, according to Newman. If they track employees' personal information, for example, they run the risk of violating privacy rights. But as long as policies are tailored with the aim of protecting the company rather than snooping on workers, courts generally won't take issue, he said.

Monitor Departing Employees

The specific practices may be different when an employee leaves than when they're still on the payroll, but the foundation is the same: Be proactive.

Experts recommend employers ask that departing employees turn over all confidential information they have, whether it be on their own device or a company device. Yonowitz also recommends that employers have workers sign what he calls a "termination certificate," stating under penalty of perjury that they have not taken any trade secrets.

“We have to demonstrate that we’ve done everything to get back information that was provided to employees so they could do their job and have evidence we did that,” Yonowitz said. “Then, if the employee took stuff, that termination certificate is wonderful because … we can show they swore they didn’t.”

This is also where monitoring software and a strong information technology group come into play. If an employer suspects an employee stole a trade secret, they need to audit the worker’s history for signs of theft.

“Take a look at the last 60 or 90 days of that employee’s computer-based activity to determine whether they have been trafficking or transferring information to personal email accounts or connecting to a hard drive,” Yonowitz said. “We also look at things like mass deletions because evidence of destruction of trade secrets is evidence of misappropriation.”

When Theft Happens, Act Fast

If these measures fail, the next step is legal action.

If the theft is as minor as an absent-minded employee simply leaving with confidential information, a simple letter asking for its return will generally do. But when the theft is believed to be willful, a lawyer becomes invaluable.

Depending on the jurisdiction, litigation options range from sending a cease-and-desist order with a draft complaint attached to filing for a temporary restraining order under state or, if the scope of the theft merits it, federal law. In extreme cases, victims of trade theft can ask for a seizure order directing authorities to take back the stolen information.

Whichever avenue an employer takes, it has to use haste because acting slowly risks damage from the leak and undermines claims of the alleged secret’s importance.

“The key here is speed,” Yonowitz said. “You can’t sit on these. As soon as you have an understanding this theft may have occurred, as an employer, you have to move quickly to demonstrate you’re making reasonable efforts to protect sensitive information.”

If it follows these guidelines, an employer can be confident that its trade secrets are safe or that they can safely be returned if taken. But with technology moving as swiftly as it does these days, employers are advised to keep close an attorney who pays attention to the trends.

"I see this area of law growing as technology and the pace of change speeds up,” said Newman, who has worked in trade secrets law for more than 20 years. “It’s never gonna slow back down.

“It’s easier than ever to store large amounts of data on smaller devices or in the cloud, and information has a value," he added. "People want to steal try to steal the most valuable things they can, and oftentimes that’s information and know-how.”

--Additional reporting by Joyce Hanson. Editing by Christine Chun and Rebecca Flanagan.
