Can Silicon Valley Keep a (Trade) Secret?

Insights
2.26.18

The simplest, most valuable, yet commonly overlooked piece of advice any trade secret owner can receive is this: Protect yours trade secrets! It seems crazy that this simple advice warrants repeating, but apparently, it does, particularly in Silicon Valley where billions of dollars have been spent researching and developing electric and autonomous vehicle technology.

EV and AV technology is undergoing a rapid transformation. AV manufacturers are preparing to test self-driving cars on our streets in the next few years. Important to this discussion, billions upon billions of dollars are being spent to win the race. If you're going to spend that type of money, it might be worth setting aside a few dollars to make sure your treasured work is yours and only yours when you cross the finish line.

Who isn't taking this approach you might ask? Some might cite Waymo and Faraday & Future as examples. If you are reading this article, you probably know about the *Waymo v. Uber* saga that recently ended with a $245 million settlement, not counting the millions of dollars spent on attorneys and other expenses, plus soft costs like lost productivity. But a brief summary is helpful.

Alphabet's self-driving unit, Waymo, sued Uber alleging that it used stolen trade secrets. Did Uber steal the trade secrets by hacking into Waymo's servers? Nope. It all began with a former Waymo employee who allegedly downloaded 14,000 files before quitting to launch his own start-up, which Uber subsequently purchased for $680 million!!

What happened with Faraday & Future? You can probably guess. After FF invested over $1 billion in developing the next generation of artificial intelligence electric vehicle technologies, it alleges that two senior, C-level executives recruited a group of FF employees to join them at their new and competing company, EVelozcity. According to FF, before leaving, multiple employees copied and "took potentially *thousands* of FF's most sensitive electronic documents from" FF computers and servers.

Starting to see a trend here?

Before addressing how this conduct can be prevented, let's spend a moment asking the question that must be on everyone's mind – why was it possible for these wayward employees to download such volumes of data on their way out the door?

According to FF, "[t]he host of trade secrets that FF has developed since 2014 would be highly valuable to any competitor in the electric vehicle space." Really? Then act like it.

Consider the Nicolas Cage movie, National Treasure. While anything is possible is possible in Hollywood, the odds that someone could successfully steal the Declaration of Independence are between slim and none. Why? Because we treat the DOI like the treasure that it is, and we take more than reasonable precautions to prevent its theft. The DOI is kept in a titanium case with bulletproof glass and is surrounded not only by inert gases, but also armed guards, countless cameras and a computerized security system. Every night, it is secured in an underground vault, and I'm willing to bet, only certain people with necessary clearance are allowed to access it. In short, we view it as a treasure, and we treat it as such. So too must we handle our trade secrets.

It is stunning to think that employees at Waymo and Farady & Future can plug in a portable storage device and make off with "valuable trade secrets." Yet, it appears that they can; and a handful of lawyers have profited handsomely as a result. So, heeding Ben Franklin's famous admonition, let's think about a few ounces of prevention that might be worth several hundred pounds of cure. In other words, how might these types of mishaps be prevented in the future? Here are a few suggestions:

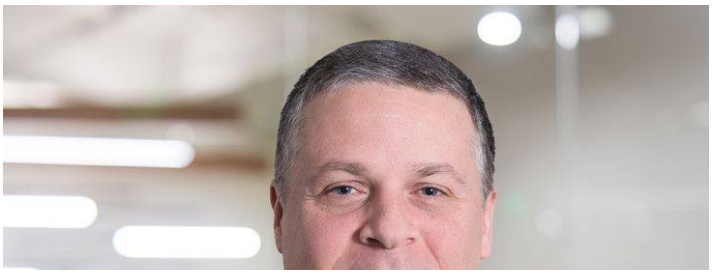
1. **Set up sufficient IT controls.** Work with your IT department or outside consultants to prevent or minimize the possibility of your trade secrets being downloaded onto a portable storage device ("PSD") or the cloud. If an employee plugs in PSD or attempts to upload data to the cloud, your system should be set up such that it won't work, and IT should receive a red flag. If for some legitimate business reason, this is not feasible, at the very least, IT should receive notification when an employee accesses thousands, hundreds or dozens of files in rapid succession (an action consistent with bulk downloading).
2. **Provide access to confidential information on a need to know basis only, and segregate information in silos when possible.** Not every employee needs to have access to every file or category of information. Limit their access to that information which they need in order to perform their duties; and to the extent possible, structure their duties so that they only know a piece of the puzzle. This way, if they leave with information, its utility is limited.
3. **Enact written policies, train your employees and let them know you're watching.** Employees who handle confidential information should be required to handle it with the care and protection it deserves. They should receive training about when, where and how it is ok to handle and use confidential information, and they should know that they must follow these protocols because their employer is watching.
4. **Use strong, well-written agreements, especially if you are in California.** Think about the risks presented if any employee were to take, use or disclose your confidential information, and make them promise in writing not to do so. But don't just use a form agreement or borrow language from the latest business-to-business NDA your company utilized. Employee agreements require careful attention. This is particularly true in California, where the use of post-employment

restrictive covenants is severely limited. You may not be able to use a non-competition agreement in California, but well-written confidentiality agreements can go a long way; and believe it or not, there are many poorly written confidentiality agreements floating around the Golden State.

5. **Conduct trade secret audits.** Conducting a trade secret audit is not a small task; but it pales in comparison (both monetarily speaking and in terms of disruption) to the litigation that arises when trade secrets are taken and used to your competitive detriment. A comprehensive audit requires a company to sit down with counsel, internal business stakeholders and IT personnel, and to some extent, external consultants in an effort to accomplish a variety of tasks. Through a proactive and systematic approach, companies must identify their trade secrets, determine who has access, how trade secrets are used, what risks are present, and how these risks can be eliminated or minimized. Potential solutions include improving and implementing written processes, training employees, preparing and rolling out effective written agreements, utilizing sufficient physical and electronic security measures, and more. Given that numerous sources estimate billions of dollars of trade secrets are stolen every year, and billions more are spent developing new secrets, businesses must spend the time and money necessary to secure those secrets. It's not a trivial expense, but it's a necessary one.
6. Exit interviews and other protocols. Trade secret theft can happen at any time, but certain events are more often accompanied by theft than others. Employee departures present such an example. Take the time to interview your departing employees and perhaps their colleagues when employees decide to move on to perceptively greener pastures. Review their recent electronic footprints and determine whether unusual electronic behavior was present.
7. **Regularly consult your legal counsel.** For the same reason you should visit your dentist for routine cleanings, make sure your outside counsel is a part of your trade secret protection plans. Don't wait until an emergency arises. The unfortunate reality in today's world is that the expense of litigation can far exceed the amount of money it costs to prevent the litigation in the first place; and if litigation ever comes to pass, you will be far better situated if you have planned for that eventuality in advance.

Michael R. Greco is a partner in the Employee Defection & Trade Secrets Practice Group at Fisher Phillips. To receive notice of future blog posts either follow Michael R. Greco on Twitter or on LinkedIn or subscribe to this blog's RSS feed.

Related People



Michael R. Greco
Regional Managing Partner
303.218.3655
Email