Articles + Publications | January 20, 2023

Water Cooler Talk: Trade Secret Lessons From ‘Severance’

WRITTEN BY

Evan Gibbs | Tracey E. Diamond | William M. Taylor

Earlier this month, President Joe Biden signed into law the Protecting American Intellectual Property Act,[1] which aims to protect U.S. intellectual property by imposing sanctions on companies and individuals involved in trade secrets theft.

Experts estimate the cost of IP theft to the U.S. economy exceeds $225 billion each year, noting it could be as high as $600 billion.[2]

Concern about protecting trade secrets is certainly not new, and the intrigue around it has trickled into popular culture, including most recently — and dramatically — in the Apple TV+ series “Severance.”

In the show, employees take a drastic step to protect their employer’s trade secrets. “Severance” features a group of people who work at a high-tech company called Lumon Industries and agree to a surgical procedure that renders them unable to remember their personal lives when they are at work or remember their work lives when they are at home.

It is the ultimate in work-life balance. Kidding!

In one scene, a character records a video explaining to her work self what has happened:

I have, of my own free accord, elected to undergo the procedure colloquially known as severance. I give consent for my perceptual chronologies to be surgically split. … I will be unable to access outside recollections whilst on Lumon’s severed basement floor, nor retain work memories upon my ascent. I am aware that this alteration is comprehensive and irreversible.

While severing employees’ work memories from their home life certainly makes it easier to control trade secrets, obviously this is not a real-life solution. The show does, however, offer several real-world takeaways for employers seeking to better protect their confidential information. Among them:

- Do not wait until sensitive data and documents are stolen to figure out what is confidential and/or a trade secret. Act now to protect confidential information to align the information with trade secret status.

- Training is critical. If company managers and employees do not know what the company considers confidential, how will they know what they can or cannot take when they leave? How will they know how to spot potential theft of critical data?

- While “Severance” is far-fetched, it illustrates that we must be careful not to go too far so that information is so encrypted that it prevents employees from understanding their job functions.

Q&A

In lieu of severing employees’ work memories, we spoke with Tim Londergan, CEO of trade secrets management software company Tangibly, about ways in which companies are working to secure their trade secrets.

Tracey Diamond: Tim, what can companies do to protect their confidential information?

Tim: It starts with documentation around the trade secret. What some recent case law teaches is that the courts are getting more specific in terms of demands, meaning there’s no longer the ability to argue this idea is institutional knowledge. It has to be documented somewhere. Step two is knowing who has access to it. Step three is ensuring that whoever has access to it — whether it’s someone inside or someone outside — has the right contracts in place to properly protect it.

Tracey: One of the greatest threats to confidentiality is employee breaches. How often is a breach inadvertent or intentional?

Will Taylor: In my litigation experience, you’re usually talking about the intentional, where somebody walks out the door with trade secrets on their laptop or briefcase. The inadvertent would be treated as a breach situation where the employee made a mistake and might be subject to some censure, including firing.

Evan Gibbs: The inadvertent stuff really does happen a lot, especially with the pandemic. I’ve had several cases where people say, “I was working from home and the VPN is slow, so I downloaded what I needed to an external hard drive.” We also hear all the time, “That’s not a trade secret. This is my document. I made it. This is mine.”

Tracey: Tim, what are your thoughts here?

Tim: Roughly 50% of trade secret misappropriation is inadvertent. People just simply don’t know. They need to understand anything they’re doing on company time is company property.

Tracey: Training is key.

Will: Training and technology. If an employer is going to make certain demands on their employees, they need to make it possible for them to do their job without violating rules about protection of information.

Tracey: The work-from-home trend is the exact opposite of “Severance.” There is such a blurring of the lines between personal life and work life, that it’s even more challenging for companies to maintain secrecy of important company data, because it’s being accessed from the home environment.

Employers are providing specific rules and work-from-home agreements about when, where and how employees perform their work so that the employer can maintain some control over it.

Evan: Tim, what do you typically find when you start working with a new client or customer?

Tim: Most customers are hacking together a solution — using a master Excel worksheet and a bunch of lawyers. Companies in the biotech and life sciences space are generally more IP-sophisticated.

Tracey: If an employer does experience a trade secret breach, how should they handle it from a litigation standpoint?

Evan: It's unfortunate, but most times you go to court and get an injunction, a temporary restraining order. We typically give the other side the heads-up and ask whoever allegedly took the information to give it back. You want to figure out if there's a way to get it without having to file a lawsuit.

Will: If you're going to enjoin an employee, collecting strong facts that support your concerns and an injunction in state or federal court is a No. 1 priority.

Conclusion

In "Severance," the company protects its trade secrets by ensuring its employees can't remember what happens to them during the workday. And while the way they do it is farfetched, the effort to protect confidential information is understandable.

Employers must strike a balance between giving employees sufficient access to sensitive materials to allow them to develop the company's IP while putting enough safeguards in place to protect the secrecy of such information.

Tracey Diamond, Evan Gibbs and Will Taylor are partners at Troutman Pepper. Diamond and Gibbs are the hosts of the Hiring to Firing Podcast.

This article is part of a monthly column that will connect popular culture to hot-button labor and employment law issues.

[1] https://www.congress.gov/bill/117th-congress/senate-bill/1294?s=1&r=59.

[2] https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report_Update.pdf.

RELATED INDUSTRIES + PRACTICES

- Labor + Employment
- Noncompete + Trade Secrets