

CLIENT ALERTS

Protecting Trade Secrets in the Automotive Industry: Federal Court Grants Tesla's Temporary Restraining Order for Trade Secret Theft

2.1.2021

On January 22, 2021, Tesla filed a trade-secret theft Complaint against a software engineer that had been with the company for just three days, serving as an important reminder to businesses that the discovery of unauthorized use of protected information requires swift action to mitigate harm.

In *Tesla, Inc. v Khatilov*, filed in the U.S. District Court for Northern California, Tesla alleges that a newly hired software engineer ("Khatilov") stole 26,000 files of code, or scripts, which automate a broad range of business functions. The Complaint alleges that, just three days following Khatilov's hire, he began downloading proprietary information from Tesla networks and onto his personal devices through DropBox. Tesla's information security team detected the download through its monitoring software. When confronted with the unauthorized downloads, Khatilov was allegedly evasive, deleted the DropBox application from his desktop, and delayed review of his desktop by Tesla's security team.

An investigation revealed that the download included complete sets of automation scripts created by Tesla's Quality Assurance Engineering Team ("QAE Team"). According to Tesla, the QAE Team is comprised of only 40 engineers out of its 50,000 employees, and only 8 of those engineers have the ability to grant access to proprietary information. The automation scripts, according to Tesla, were "highly confidential" and proprietary in nature. Tesla alleged that it has spent roughly "200 man-years of work" to develop the scripts, which is the cumulative hours spent by the QAE Team over the past 12 years. Developing the scripts was expensive and time consuming, but more importantly, access to the scripts would enable competitor companies to reverse engineer its proprietary processes to copy Tesla's innovation. Those competing companies would not be able to recreate the scripts based on public information alone.

Related People

Javon R. David
Shareholder

Related Services

Litigation and Dispute
Resolution

Non-Compete & Trade Secret

Trade Secret & Non-Compete
Specialty Team

CLIENT ALERTS

Tesla's Complaint further alleges that it takes extensive measures to ensure Tesla trade secrets remain confidential, including requiring employees to sign confidentiality and non-disclosure agreements upon hire. The non-disclosure agreement signed by Khatilov prohibited the use or disclosure of proprietary information, including technical data. In addition, Khatilov signed an Internet Usage Policy that prohibits "transmitting, copying, downloading, or removing trade secret, proprietary, or confidential business information of Tesla without written authorization." In light of the governing agreements, Tesla filed suit for Trade Secret Misappropriation and Breach of Contract.

Concurrent with its Complaint, Tesla filed an Emergency Motion for Temporary Restraining Order to Prevent Further Trade Secret Misappropriation ("TRO Motion"). The court granted Tesla's TRO Motion, finding that (1) there is a substantial likelihood that Tesla will succeed on the merits of its claims for misappropriation of trade secrets and breach of contract for the unauthorized download of documents; (2) absent a temporary restraining order in place, Tesla will suffer immediate and irreparable harm due to the employee's use and disclosure of trade secrets; (3) the balance of hardships favor entering a restraining order because the harm to Tesla substantially outweighs the cost to the employee; and (4) there is a strong public interest in favor of protecting trade secrets. The court also ordered Khatilov to appear for a hearing and demonstrate why a preliminary injunction should not be entered against him.

The *Tesla* case highlights judicial commitment to the protection of trade secrets. In addition, the *Tesla* case illustrates important lessons for businesses in the protection of trade secrets: (1) ensure that there are safeguards in place to protect confidential and/or proprietary information; (2) limit the number of individuals with access to such information; and (3) if it is discovered that an individual has taken steps to misappropriate proprietary and/or confidential information, act swiftly to mitigate the potential harm. The Butzel Trade Secret Team stands ready to help you prosecute the unauthorized use of protected information.

Javon David

248.258.1415

davidj@butzel.com