LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com

WEDNESDAY, APRIL 20, 2022

REFERRING TRADE SECRET THEFT TO THE DOJ: PRACTICAL CONSIDERATIONS

2022 INTELLECTUAL PROPERTY | BY JAY NEUKOM, LISA ZORNBERG AND DANIEL JOINER

Companies victimized by trade secret misappropriation are turning not just to civil litigation as a remedy but also, frequently, to the Department of Justice for a criminal investigation and possible prosecution. This article addresses a handful of issues that should be considered before a trade secret owner makes a criminal referral to the DOJ.

First, a reality check: most instances of trade secret theft will not be criminally investigated or prosecuted, even if referred to the DOJ. That is in large part a reflection of the DOJ's and the FBI's limited resources and prosecutorial discretion. Indeed, in 2016 Congress established a federal, civil private right of action for trade secret theft (passing The Defend Trade Secrets Act) to make it easier for companies to civilly pursue these cases on their own. Absent a "plus factor" that makes the case particularly compelling, criminal authorities are unlikely to take on the most prevalent fact pattern for trade secret misappropriation – an employee migrates company files to a personal device or personal account while preparing to leave and join a competitor.

So what "plus factors" are likely to garner DOJ attention and warrant criminal prosecution? Here are several:

- *A foreign state is benefitting from U.S. trade secrets.* E.g., the U.S. Attorney in eastern Missouri prosecuted Haitao Xiang for allegedly conspiring to steal trade secret information from a St. Louis company for the purpose of benefitting the People's Republic of China. Most of the criminal trade secret prosecutions in the last four years involved a nexus to China under the DOJ's now-disbanded "China Initiative." Even though the Biden administration scrapped the name "China Initiative," trade secret thefts with a nation-state nexus – to Russia, China, North Korea and Iran or beyond – remain of high interest to the DOJ.
- *The trade secret theft was accomplished by cyberattack.* E.g., the U.S. Attorney in the District of Columbia prosecuted Chinese computer hackers and Malaysian businesspeople who stole source code from the electronic communications industry and other industries using cyber tactics. Thefts of intellectual property facilitated by "hacking" raise national security implications for U.S. infrastructure that are a high DOJ priority. "Hackers" can be company insiders too – who use cyber tactics to gain unauthorized access to their employers' trade secrets.
- *The victim is an especially prominent company and/or operating in an economically key industry.* E.g., the U.S. Attorney in northern California prosecuted Anthony Levandowski for allegedly stealing self-driving-car trade secrets from Waymo, an Alphabet subsidiary.

This list of "plus" factors is not exhaustive. Nor should victims be discouraged from seeking the assistance of criminal authorities for serious theft cases. But given the proliferation of serious yet "run-of-the-mill" theft cases – where a U.S. employee improperly took customer-list files or code while moving from one Silicon Valley SaaS competitor to another – companies should not be surprised if their referral is met with a response of "that is terrible, and you should pursue that civilly."

Second, if choosing to make a criminal referral to the DOJ: How and when should that be done? A trade secret victim hoping for DOJ action should (i) contact its local U.S. Attorney's office (ideally, the specific Assistant U.S. Attorney or unit chief handling the trade secret docket) to request an in-person meeting; and then (ii) be prepared to present sufficient evidence to address all aspects of the case. E.g., a company should be prepared to show evidence that it takes reasonable efforts to protect the secrecy of its information; that such information truly is secret; that such information derives value by virtue of being unknown to competitors; and evidence (the more granular and clear the better) that the alleged perpetrator unlawfully accessed, used or disclosed the subject information. This presentation should be handled with care given that the DOJ will want to discuss frankly not just the strengths of a potential case but also its weaknesses, and such communications between a company and the DOJ are not privileged.

For timing, the short answer is that a company should generally approach the DOJ once having sufficient evidence to support a criminal investigation, if not charging. That may be before commencing civil litigation, or during the course of a pending civil case, depending on whether a company is able to procure sufficient evidence of actionable wrongdoing without discovery. This requires strategic consideration, particularly as certain law enforcement tactics to investigate trade secret theft (search warrants, recorded calls, undercover operations) may be effective only if undertaken before the conduct has been "outed" through a civil suit.

Third, if a company makes a criminal referral to the DOJ for trade secret misappropriation, that may have substantial consequences for a corresponding civil lawsuit. Examples of such consequences include:

- The individual defendant in a civil lawsuit for trade secret misappropriation, if aware of a criminal investigation or prosecution, could decline to provide testimony or personally held documents by invoking the Fifth Amendment right against self-incrimination. (Corporations, however, cannot "take the Fifth.")
- For purposes of managing its criminal investigation or prosecution, the DOJ may ask the victim company to delay filing civil claims for trade secret misappropriation or, if such claims are already pending, to stay the civil case.

Whether these or other consequences on civil litigation are material enough to a victim of trade secret misappropriation to deter a criminal referral will of course depend on the victim's objectives. For those more interested in emergency relief against a competitor (such as through a TRO in a civil case), or maximizing monetary damages in a civil case, these kinds of consequences may weigh against a criminal referral.

Jay Neukom is a partner in Debevoise & Plimpton LLP's Intellectual Property Litigation Group based in San Francisco. He is a veteran trial lawyer with extensive experience advising major Bay Area companies on complex business and intellectual property disputes, including trade secret misappropriation, and patent and copyright infringement matters.

Lisa Zornberg is a partner in Debevoise & Plimpton LLP's White Collar & Regulatory Defense Group in New York and former Chief of the Criminal Division for the U.S. Attorney's Office for the Southern District of New York. Her practice focuses on white collar defense, regulatory enforcement actions and internal investigations as well as complex civil litigation.

Daniel Joiner is an associate in the Litigation Department at Debevoise & Plimpton LLP.