

# When To Call The Feds For Trade Secret Theft Investigations

FEBRUARY 6, 2019

*This article originally appeared in [Law360](#). Reprinted with permission. Any opinions in this article are not those of Winston & Strawn or its clients; the opinions in this article are the authors' opinions only.*

A company suspects that an employee, a former employee, or a manufacturing or development partner has stolen its valuable trade secrets. What can and should the company do?

While many companies in this situation conduct internal investigations geared toward seeking civil remedies, such as a temporary restraining order, a permanent injunction and/or damages, companies seem to overlook—or intentionally shy away from—referring such matters to law enforcement. But in some circumstances, using the criminal justice system can be more effective than using civil lawsuits or internal procedures alone, particularly given the powerful investigative tools law enforcement can deploy and the potential deterrent effect a criminal case can have on similar future conduct.

This article discusses the types of trade secrets cases that the U.S. Department of Justice has prosecuted, and the potential benefits and drawbacks of seeking law enforcement assistance.

## **Analysis of Federal Trade Secret Prosecutions**

While a study by Symantec (alarmingly) found that 44 percent of respondents did not think it is a crime to use a competitor's trade secrets, in fact, it is.<sup>[1]</sup> The Economic Espionage Act, codified at 18 U.S.C. § 1831 and 18 U.S.C. § 1832 prohibits stealing, sharing, or receiving a misappropriated trade secret. Importantly, however, the DOJ does not—and cannot—pursue each and every instance of corporate trade secret theft; it must pick and choose. Therefore, it is important for counsel—both in-house and external—to understand the types of cases the DOJ prosecutes.

Although the DOJ does not currently provide statistics or publicly track theft of trade secret prosecutions, we have identified, through various sources, 184 federal prosecutions under 18 U.S.C. § 1831 and § 1832 from 1997 to November 2018.<sup>[2]</sup> We have analyzed these cases with an eye toward identifying factors that the DOJ likely focused on when deciding whether to bring a criminal case.

Notably, national and international politics and priorities play a role in setting DOJ priorities and defining what types of prosecutions further a “federal interest.” Under President Donald Trump's administration, the DOJ has been

particularly focused on trade secret theft involving Chinese entities. On Nov. 1, 2018, then-Attorney General Jeff Sessions announced an initiative to “identify priority Chinese trade theft cases, ensure that [there are] enough resources dedicated to them, and make sure that we bring them to an appropriate conclusion quickly and effectively.”[3] In 2017 and 2018 alone, there were at least nine cases that alleged that information was stolen from American companies to benefit a Chinese entity.[4]

Sophistication of DOJ resources and priorities of local offices also impacts which cases are pursued. Of the 184 cases we reviewed from 1997 through 2018, the top five states where federal prosecutors have brought trade secret cases are as follows: California (52 cases), New York (17 cases), Texas (12 cases), Pennsylvania (10 cases), and Ohio (10 cases). Of course, these numbers alone do not explain whether these higher rates of prosecutions correspond to a higher rate of trade secret theft in those states, a prioritization of such cases by the local federal prosecutors located in those states, or other factors.

It should also be noted that while Wisconsin did not make the top five in terms of number of cases, the per-capita number of cases there is high; there have been at least seven trade secret prosecutions since 1997 in Wisconsin, four of which were charged within the past six years alone, even though the state has a comparatively low population.[5]

Although the DOJ will follow certain guiding principles when assessing what trade secret cases to pursue (e.g., deterrence of future malfeasance and protection of the public), there is no uniform type of trade secret case: the victims of trade secret theft span across industries, and the types of trade secrets stolen are diverse. For example, the secrets at the heart of recent federal trade secret prosecutions have ranged from algorithmic data relating to high frequency trading,[6] to engineered rice seeds,[7] to technology used to create random access memory chips for computers.[8] That said, the data suggests that the feds are more likely to bring a case that involves highly valuable trade secrets.

While prosecutors cannot predict the outcomes of the prosecutions, the data shows that there is not a uniform tendency to only prosecute cases that result in significant sentences. Indeed, sentences for individuals convicted of trade secret theft vary significantly.

For example, in 2014, a defendant who admitted to emailing specifications for brake pads from his employer to a foreign company was sentenced to three years of probation and had to pay \$23,000 in restitution.[9] On the other end of the spectrum, a defendant was sentenced to serve 15 years in prison, forfeit \$27.8 million in illegal profits, and pay \$511,667.82 in restitution in 2014. There, the defendant conspired to steal trade secrets from E.U. du Pont de Nemours & Company relating to their production technology and sell them to state-owned companies in China. [10]

The differences in sentences may be based on, among other factors, what the defendant planned to do with the stolen trade secrets, as well as the amount of loss caused by the theft. The latter is a figure that can drive the sentencing guidelines range, but can be challenging to calculate in trade secret cases.

### **Pros and Cons of Referring a Trade Secret Case to Law Enforcement**

Referring a theft of trade secret matter to law enforcement can benefit a company in many ways. As outlined below, not only does the federal government have evidence collection powers that stretch well beyond a company’s capabilities, but using the justice system may have a higher deterrence effect to ward off future offenders, and cost a company less in the long run.

Compared to a private company, the FBI and DOJ have broad investigative powers that can be particularly beneficial in theft of trade secret matters.

The FBI can execute search warrants and seize devices that may contain stolen trade secrets. These tools not only provide key evidence that the company would not be able to gather, but also help prevent further use or disclosure of the trade secret. Authorities also employ, under court supervision, investigative techniques to contemporaneously monitor movements and communications of suspects, including real-time monitoring of phone

calls, text messages, emails, and tracking of vehicles and personal movements. This can provide valuable insights into the suspect's activities, as well as reveal co-conspirators.

Additionally, the DOJ can serve grand jury subpoenas to preserve or collect key evidence from third parties that are not under the victim company's control, including electronic evidence. The DOJ can also compel testimony from witnesses or individuals who are unwilling to cooperate. Furthermore, the Department of Justice has resources to conduct and gather evidence and testimony and restrain assets abroad. In some circumstances, the Department of Justice may gather evidence—in the U.S. or abroad—that helps a company get its data back and prevents its dissemination, even if the investigation does not lead to a prosecution.

Given the options in the government's toolbox, cooperation with law enforcement can result in more effective investigations, which can in turn allow companies to protect their data—and potentially obtain its return—in ways they would not otherwise be able to do. For example, GE Aviation benefited last year from cooperating with law enforcement when a Chinese intelligence agent conspired to steal trade secrets from multiple U.S. aviation companies, including GE Aviation.[11] After prosecutors indicted the alleged thief, a GE Aviation spokesman explained that “[t]he impact to GE Aviation [was] minimal thanks to early detection, our advanced systems and internal processes, and our partnership with the FBI.”[12]

Similarly, the company Phillips 66 found evidence of potential trade secret theft after reviewing an employee's computer following his resignation. The company referred the matter to the FBI. The FBI discovered ties between the employee and a Chinese company, which offered to pay him \$50,000 for “talent” he would bring to the company. The employee was arrested and is currently being held without bail pending charges.[13]

Referring a matter to law enforcement—and doing so quickly—may also decrease the costs a victim company ultimately pays to protect its assets. In the past, courts in many jurisdictions allowed companies to recover costs of their internal investigations through restitution judgments. However, the U.S. Supreme Court recently concluded in *Lagos v. United States* that under the Mandatory Victim Restitution Act, costs incurred in an investigation that a “victim chooses to do on its own” cannot form the basis of a restitution judgment.[14] As such, following *Lagos*, a company may only be able to recoup costs it incurred cooperating with law enforcement's investigation or prosecution. Thus, a company increases its chances of recovering its investigation costs when it refers a matter to law enforcement, rather than conducting a costly internal investigation on its own accord.

Securing a criminal conviction, or even just bringing criminal charges, can also have a deterrent effect that civil litigation alone may not have, particularly for cases where the defendant is an employee. Such deterrence spreads not only to employees of the victim company, but also outside employees in the same industry or jurisdiction. This deterrence impact is often the most effective way to prevent theft, as ever-resourceful employees are constantly coming up with new and clever ways to steal volumes of data that stay one step ahead of theft detection systems.

There is also a “good corporate citizen” aspect to the referral decision. Many companies proudly tout their corporate values, their corporate social responsibility, and the company's desire to “do the right thing.” Companies faced with the unenviable position of having concluded that someone has stolen valuable information from them must decide how the corporate response to that situation aligns with the values that the company tells its employees to live by.

Along the same lines, the DOJ benefits from corporate cooperation: Companies are on the front lines and may be able to bring potential cases to the government's attention. This allows the government to assess whether there is a broader interest—such as international espionage—that needs to be addressed. For years the DOJ has been engaged in corporate outreach initiatives, encouraging companies to bring cases to their attention. Most recently, FBI Director Christopher Wray gave a speech encouraging companies to cooperate with the DOJ in cases involving cyberthreats and theft of trade secrets, both before and after malfeasance is suspected.[15]

For all of the potential upsides to referral, there are both real and perceived downsides as well. For starters, some companies do not want to invite the feds in to investigate trade secret theft, for fear of “letting the tiger loose” and giving the feds free rein to rummage through the company's files and systems in search of unrelated wrongdoing. While that fear is understandable, there are some important clarifications to consider. The DOJ and FBI have made

clear that they view victim companies as victim companies and do not use these types of actions as subterfuge to investigate a company for something else. In the collective experience of these authors, and our colleagues, that is universally the case.

Notably, much of the investigation of company information, documents and witnesses will be conducted in the first instance by, or at least supported by, the company's own lawyers. Like in the context of other types of internal investigations (e.g., fraud or Foreign Corrupt Practices Act), the bulk of internal review will likely be conducted by trusted outside counsel. Often, these are former DOJ lawyers who work at the direction of the company or the board to conduct the investigation thoroughly, but also in the least disruptive manner possible. As such, a team of FBI agents running amok through the company hallways is not the reality.

There are, however, other potential downsides to referring these cases to the government. First, once law enforcement is driving the investigation and prosecution, the company is no longer in control. Second, trade secret prosecutions require significant resource investment from the victim company, which may be required to produce documents in response to a grand jury subpoena, have employees sit for interviews with the FBI, and have employees testify at a trial. Third, proving a trade secret case requires proof of what the trade secret is, with some level of specificity, which may not be information the company wants to share, even if the disclosure will be protected from dissemination at trial. Finally, a victim company may not want to admit publicly that it had information stolen, as that may call into question its security protocols or otherwise be damaging to the company from a public relations standpoint.

Given the varying costs and benefits of a referral, there is no one-size-fits-all answer to the "refer or not to refer" question. But, companies should not automatically reject the idea of referring matter to law enforcement, particularly in the trade secret context where proving theft can be challenging, and acting swiftly is key. Thinking through the pros and cons, and considering the types of cases the DOJ has focused on, early in the company's internal investigation will help ensure that the victim company makes the right decision and improve the chance that a referral to law enforcement will be successful.

---

[1] See, Symantec, Symantec Study Shows Employees Steal Corporate Data and Don't Believe It's Wrong, Feb 6, 2013, [https://www.symantec.com/about/newsroom/press-releases/2013/symantec\\_0206\\_01](https://www.symantec.com/about/newsroom/press-releases/2013/symantec_0206_01).


[2] Trade secret theft may also be prosecuted under other statutes, such as the mail or wire fraud statutes or the Computer Fraud and Abuse Act.

[3] Attorney General Jeff Session's China Initiative Fact Sheet, Nov. 1, 2018, Department of Justice.

[4] See, United States v. Liu Xuejun (case number unknown, indictment filed Aug. 3, 2018); United States v. Xioqing Zheng (No. 18 Mj. 00434); United States v. Xiolang Zhang (No. 18 Cr. 70919); United States v. Liang Chen et. al. (No. 17 Cr. 00603); United States v. Yingzhuo Wu (No. 17 Cr. 00247); United States v. Jerry Jingdong Xu (No. 17 Cr. 00063); United States v. Shan Shi (No. 17 Cr. 00110); United States v. Dmitry Dokuchaev, et. al. (No. 17 Cr. 00103); United States v. Gregory Allen Justice (No. 17 Cr. 00499); United States v. Yanjun Xu (No. 18 Cr. 43); United States v. United Microelectronics Corp., et. al. (No. 18 Cr. 465).

[5] In 2017, the population in Wisconsin was 5.795 million. Comparatively, it was 39.54 million in California, 8.623 million in New York, 12.81 million in Pennsylvania, and 11.66 million in Ohio. United States Census Bureau, <https://www.census.gov/en.html>.

The seven Wisconsin cases are: United States v. Tan Liu (No. 16 Cr. 00079); United States v. Sinovel Wind Group (No. 13 Cr. 00084); United States v. Jun Xie (No. 14 Cr. 00205); United States v. Huajun Zhao (No. 13 Cr. 00058); United States v. Koval (No. 04 Cr.00061); United States v. Conti et. al. (No. 05 Cr. 0151) and United States v. Lange (No. 99 Cr. 00174).

[6] United States v. Yihao Pu, et. al.  (No. 11 Cr. 00699).

[7] United States v. Liu Xuejun (No case number has been located); for further reference see <https://www.justice.gov/usao-edar/pr/chinese-nationals-charged-conspiracy-steal-rice-technology>.

[8] Jeff Sessions, Former Attorney Gen., Attorney General Jeff Sessions Announces New Initiative to Combat Chinese Economic Espionage (Nov. 1, 2018); See also, United States v. United Microelectronics Corp. (No. 18 Cr. 00465).

[9] United States v. David Lewis (No. 14 Cr. 00014).

[10] See Dep't. of Justice, Walter Liew sentenced to Fifteen Years in Prison for Economic Espionage, July 11, 2014, <https://www.justice.gov/usao-ndca/pr/walter-liew-sentenced-fifteen-years-prison-economic-espionage>.

[11] See, Michael Balsamo and Angie Wang, "Feds: Chinese spy tried to steal US aviation trade secrets," Associated Press, Oct. 10, 2018, <https://www.apnews.com/95d58154c0664f1f999e4d26781afefd>.

[12] Id.

[13] See, United States v. Hongjin Tan (No. 18 mj 00179); See also, <https://www.justice.gov/opa/pr/chinese-national-charged-committing-theft-trade-secrets>.

[14] See, Lagos v. United States , 138 S. Ct. 1684 (2018).

[15] Christopher Wray, Director, Fed. Bureau of Invest., Address at The National Association of Corporate Directors Global Board Leaders Summit: The FBI and Corporate Directors: Working Together to Keep Companies Safe from Cyber Crime (Oct. 1, 2018).

10+ Min Read

## Related Locations

Chicago

## Related Topics

Trade Secrets

Law360

## Related Capabilities

Litigation/Trials

Privacy & Data Security

Trade Secrets, Non Competes & Restrictive Covenants

Compliance Programs

Technology, Media & Telecommunications

Financial Services

## Related Regions

North America

## Related Professionals

---



Steven Grimes