KAYE | SCHOLER

Bylined Article

Trade Secret Theft and Corporate Espionage: Tips for Prevention and Response

Z Scott and **Elizabeth Pozolo**

A version of this article originally appeared in two parts in InsideCounsel *on April 22, 2014 and May 20, 2014.*

The Federal Bureau of Investigation (FBI) estimates that every year billions of US dollars are lost to foreign and domestic competitors through corporate espionage leading to the theft of valuable trade secrets. Resources from the top levels of the US government are focusing on this growing problem. Last year the White House issued a report outlining a new strategic plan to combat trade secret theft from US businesses, stating that "[t]rade secret theft threatens American businesses, undermines national security, and places the security of the US economy in jeopardy."

Just who are these thieves that are compromising US trade secret assets? According to the FBI, in many instances they are not outsiders but instead are corporate employees working within companies that have been targeted and compromised by outsiders. It is imperative that US companies understand how the theft of intellectual property assets routinely occurs and have knowledge of the laws, resources and processes that are available to protect and defend against the theft.

Recent criminal trade secret investigations and cases

The methods used to compromise US trade secret assets are broad and varied, but the cases and investigations do reveal a few common denominators, making a summary of these cases instructive.

In some reported instances, for example, the criminal conduct of corporate employees or their accomplices was exposed as they went through examinations by US Customs entering or leaving the US. The stolen trade secrets were often captured on a portable electronic device such as an external hard drive or laptop. The implicated employee may be traveling to high-risk countries during employment and, at times, downloading massive amounts of data from company systems before or after the travel.

A recent case involving theft from telecommunications corporation Motorola further illustrates these points. In February 2007, former Motorola software engineer Hanjuan Jin walked on the jet bridge to board a flight to Beijing from Chicago's O'Hare International Airport. She had a one-way ticket and was scheduled to begin a new job with another telecommunications company in China. A US Customs officer stopped her as part of a random check of passengers. A search revealed that Jin was carrying $30,000 in cash in her laptop bag and her carry-on bags contained Motorola documents considered proprietary cellular telecommunications technology and marked "confidential and proprietary information."

Jin was later prosecuted by the federal prosecutors for theft of Motorola's trade secrets and violation of the Economic Espionage Act (EEA), an important federal criminal statute that prohibits the misappropriation of trade secrets. In a bench trial, she was convicted of theft of trade secrets and acquitted of the EEA charges. While the judge concluded that there was insufficient evidence to conclude that Jin's theft intended to benefit the Chinese government, he found that the evidence in this regard was compelling enough to enhance her prison term. At sentencing, he concluded that under the applicable US Sentencing Guidelines, her conduct not only involved "misappropriation of a trade secret," it further involved an intent to benefit a foreign government, foreign instrumentality, or foreign agent." Jin received a four-year sentence, reported to be one of the harshest ever levied in a trade secret theft case.

"Just who are these thieves that are compromising US trade secret assets? According to the FBI, in many instances they are not outsiders, but corporate employees working within companies that have been targeted and compromised by outsiders."

Early last year, federal prosecutors indicted Sinovel Wind Group Co., a manufacturer and exporter of wind turbines based in the People's Republic of China for theft of trade secrets from its former US supplier American Semiconductor Corp (ASC). The indictment, which charges the company with criminal conspiracy, trade secret theft and wire fraud, alleges that Sinovel, through two of its executives, recruited an ASC employee to leave ASC and join Sinovel, and to secretly copy intellectual property from the ASC computer system. This case further illustrates the point that often the point of compromise of an employee comes from outside of the company.

The case was investigated as part of the Department of Justice Task Force on Intellectual Property (IP Task Force). In announcing the indictment in the *Sinovel* case, FBI Executive Assistant Director Richard McFeely stated this case "is a classic example of the growing insider threat facing our nation's corporations and their intellectual property." An equally important message delivered by McFeely was that, "[t]he FBI will not stand by and watch the hemorrhage of US intellectual property to foreign countries who seek to gain an unfair advantage for their military and their industries. We are actively working with our private sector and government

partners to disrupt and impact those who have made it their mission to steal US military and corporate secrets. Since 2008, our economic espionage arrests have doubled; indictments have increased five-fold; and convictions have risen eight-fold."

The Economic Espionage Act was used by federal prosecutors in both the *Jin* and *Sinovel* cases. The EEA outlaws two categories of trade secret theft: theft for the benefit of a foreign entity (economic espionage) and theft for pecuniary gain (theft of trade secrets). To qualify as a "trade secret" under the EEA, the owner of the secret must have "taken reasonable measures to keep such information secret." Whether an owner has taken reasonable measures to ensure the secrecy of his or her trade information will depend upon the circumstances of the case. However, at a minimum, these measures should include limiting access to the information and notifying employees of its confidential nature. These simple but necessary security measures are also crucial to preventing the theft of secrets in the first place.

"The Economic Espionage Act outlaws two categories of trade secret theft: theft for the benefit of a foreign entity (economic espionage) and theft for pecuniary gain (theft of trade secrets)."

Of course, prevention will not always be possible. In *Jin*, the district court concluded that Motorola's "multi-pronged approach to security — controlled and monitored physical access to Motorola facilities, limited access to the Motorola computer network and Motorola network equipment, a specific policy for the protection of proprietary information, and confidentiality agreements and trainings for Motorola employees — was a reasonable way to maintain the secrecy of the information." Yet Jin, as noted above, was able to circumvent these precautions.

Just as trade secret theft and corporate espionage have certain fact patterns that tend to come up again and again, so do the actions of companies that often succeed in combating these challenges. These companies regularly evaluate the compliance controls in place, and also remain poised to respond immediately in the event a trade secret theft occurs.

The threat of trade secret theft from US businesses is real and complex. No business sector is immune. Understanding the nature of the problem with a keen focus on a strong compliance culture and accessing the available government resources can assist companies in managing this risk. Companies should also be poised to access the civil and law enforcement resources available to them if a threat occurs. Congress, the White House and federal law enforcement agencies have prioritized the investigation and prosecution of trade secret theft. In announcing the Administration's strategic plan to combat trade secret theft, US Attorney General Eric Holder stated that there are only "two categories" of companies affected by trade secret theft — "[T]hose that know they've been compromised and those that don't know yet."

With trade secret theft against US corporations on the rise, the government has promised an increase in enforcement efforts using existing laws and two new federal laws designed to strengthen the Economic Espionage Act (EEA). More specifically, the Theft of Trade Secrets Clarification Act of 2012 expands the EEA's coverage beyond products sold in interstate or foreign commerce and clarifies that the EEA also applies to trade secrets relating to products and services that a company uses internally. The Foreign and Economic Espionage Penalty Enhancement Act of 2012 increases the maximum penalties for the theft of trade secrets with an intent to benefit a foreign government or instrumentality. For organizations, the maximum fine is now either $10 million or three times the value to the organization of the stolen trade secret.

Below are some tips that companies can take proactively to help prevent the loss of these valuable corporate assets. However, as thieves can foil even the most robust attempts at deterring them, we also summarize steps that companies can take if, despite their best efforts, they become the victim of this common and damaging crime**.**

"Understanding the nature of the problem with a keen focus on a strong compliance culture and accessing the available government resources can assist companies in managing this risk."

Tips to prevent theft of trade secrets

#1: Cut off or tighten access: Many employees are using portable devices to store and save proprietary data, and corporate e-mail systems are not properly protected. One way to hamper the use of thumb drives and other external devices is to place limitations on the amount of data that can be electronically copied, and possibly even disable the use of USB and DVD ports on employees' computers entirely. Companies should also enhance their information security policies by requiring multiple passwords and maintaining thorough records of who is accessing certain networks and downloading files.

#2: Create a culture of compliance: In addition to taking steps to tighten IT security, companies must also prioritize compliance and training programs that educate employees' possibilities of compromise from foreign governments, the existence of the EEA, and its penalties. Companies should establish clear guidelines for what constitutes a trade secret and make employees aware that the company's policy requires them to report suspicious behavior by co-workers, supervisors and direct reports. Having an anonymous compliance hotline in place will encourage employees to report illicit trade secret activity that may save the company from criminal liability down the road. Companies should not underestimate the need for a strong compliance program and policies in this area. Recently, a US company entered into a non-prosecution agreement with the US Attorney's Office settling allegations of trade secret theft and accepting responsibility for their actions and pledging to continue a culture of corporate compliance.

#3: Hire carefully: Companies may not be aware that they could be subjected to an enforcement action for theft in this regard if stolen trade secrets find their way into their companies. The EEA allows for the prosecution of a company that "receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained or converted without authorization." Thus, a company can be on the hook for violation of the EEA even if it did not steal the secret — it is enough that one of its employees encountered the secret information in the course of his work. As a compliance measure, therefore, when on-boarding new employees from competitors, particularly if the new employees were all part of team or group with a competitor, care should be taken to make sure that there is a documented business need for the hire and trade secrets learned in the prior job do not creep into the new employer's systems.

"A company can be on the hook for violation of the EEA even if it did not steal the secret — it is enough that one of its employees encountered the secret information in the course of his work."

#4: Exit right: Last, companies should have a substantive and robust exit interview of departing employees who had access to confidential and proprietary information. Securing detailed information from employees as they leave for a competitor can prove helpful to civil or criminal enforcement remedies down the road.

Responding if a breach occurs

What steps should a company take if, despite its best efforts, a trade secret breach occurs?

#1: Commence an investigation: Immediate action is required and necessary. The company should immediately commence an investigation to determine the identity of the culprit and the breadth of the compromise. If a civil lawsuit is contemplated, the law requires that the company provide specific information identifying the threat and compromise.

#2: Seek back-up: If criminal resources are needed, enlist the support of the Federal Bureau of Investigation. The FBI has made intellectual property theft a priority in its criminal investigative program. Using the EEA and other federal laws, federal law enforcement can reach and investigate conduct that occurs outside the US involving both products or services intended to be used in interstate commerce. Moreover, the Department of Justice has assembled a Task Force on Intellectual Property that is part of a Department-wide initiative to confront the growing number of domestic and international intellectual property crimes. The Task Force is chaired by the deputy attorney general.

#3: Consider filing an ITC claim: If the theft occurs outside the US, a company should also consider filing a claim with the US International Trade Commission (ITC). As evidenced by an

increase in recent filings before the ITC, it has become a popular forum for combating international trade secret theft as a result of a Federal Circuit decision affirming that Section 337 of the Tariff Act of 1930 applies to trade secret misappropriation where the unfair act occurs exclusively outside the US In order to bring a successful trade secret misappropriation case before the ITC, a claimant must establish the existence, ownership and compromise of a trade secret together with evidence of importation of an item or the sale of imported articles that utilize the trade secret.

While the remedies before the ITC do not include money damages, another powerful tool is available: an exclusion order enjoining the respondent from importing the offending articles into the United States and/or a cease and desist order enjoining domestic manufacture or sale of the relevant articles by the respondent within the United States. It is important to note that an ITC exclusion order is enforced by federal agencies such as US Customs and Border Protection and blocks the US importation of any of the goods incorporating — or even manufactured in accordance with — the misappropriated trade secrets. In addition, ITC cases move fairly quickly and must be concluded within 16 months.

Even the most sophisticated companies can fall victim to trade secret theft. Therefore, it is essential for all companies to regularly evaluate their security systems and compliance programs and become educated on the various ways in which thefts occur, so that they may prevent them from happening in the first place.

About the Authors

Z Scott
+1 312 583 2347
z.scott@kayescholer.com

Z Scott is a partner in Kaye Scholer's White Collar Litigation & Internal Investigations Practice in Chicago. She concentrates her practice on complex commercial litigation, corporate internal investigations (including matters related to the Foreign Corrupt Practices Act), counseling on corporate compliance matters and white collar criminal defense.

Elizabeth Pozolo
+1 312 583 2435
elizabeth.pozolo@kayescholer.com

Elizabeth Pozolo is a litigation associate in Kaye Scholer's Chicago office. She has significant experience in complex commercial litigation matters, class actions and corporate internal investigations.