Outside Counsel

Referring Trade Secrets Theft for Criminal Prosecution

Guy Singer, Mark Mermelstein and Mary Kelly Persyn, New York Law Journal

June 10, 2014

Cybercrime—including trade secrets theft—has famously been termed "the greatest transfer of wealth in human history" by recently retired National Security Agency head General Keith Alexander. See "The Next Wave" [NSA] 19:4 (2012). Corporate victims of trade secrets theft will hardly disagree. Ex-employees who depart with cyber-secrets stuffed in their figurative pockets cost industry a staggering, and annually increasing sum currently pegged at $250 billion per year. See "NSA Chief: Cybercrime constitutes the 'greatest transfer of wealth in history,'" The Cable (July 9, 2012).

Universal dependence on advanced technology means that intellectual property is the lifeblood of most modern corporations, and its theft is potentially debilitating. Upon discovery of suspected theft, the temptation to seek criminal prosecution under the federal Economic Espionage Act as retribution and deterrence can be overwhelming. But corporate counsel do well to pause, consider carefully, and consult outside counsel with broad criminal law experience before turning to the United States with a criminal referral.

Evidence that an employee violated company trade secrets policy or a confidentiality agreement is simply insufficient, without more, to put together a successful criminal referral and prosecution. Outside counsel evaluating possible referrals should note Department of Justice policy requiring "aggravated conduct" in order to prosecute trade secrets theft, including acts like selling valuable trade secrets to the highest bidder; working on a prototype product and then launching a new business based on that product; and accessing company information to fulfill an international contract (not for the employer). Conduct like leaving employ and taking files or data along, may not suffice on its own, to merit criminal prosecution. Other factors that the Justice Department will use to evaluate a case include the "degree of economic injury to the trade secret owner; the type of trade secret misappropriated; the effectiveness of available civil remedies; and the potential deterrent value of the prosecution." Justice Department, U.S. Attorneys' Bulletin 57:5 at 5 (2009), citing USAM Sec. 9-59.100. The question is not whether wrongful conduct occurred, but whether the conduct warrants criminal prosecution.

Scrutinizing Cases

While the first question is the egregiousness of the conduct, referring counsel have several more sets of inquiries to pursue, including legal, strategic, and ethical approaches. If the intent is to refer to the U.S. Attorney's Office, the relevant statute is the Economic Espionage Act. See 18 U.S.C. §§1831-1839.

Section 1832 criminalizes five types of misappropriation, including theft/fraud, copying, possession/purchase, attempt, and conspiracy, when done with the knowledge or belief that a trade secret is involved and with the intent to benefit a third party and to injure the trade secret owner. In deciding whether to make a criminal referral to the Justice Department, the legal evaluation of the case should focus primarily on the key elements that distinguish criminal trade secrets theft from civil misappropriation: intent to convert the secret for the economic benefit of a third party; and intent to injure the trade secret owner. See 18 U.S.C. Sec. 1832(a).

California corporation Broadcom learned this painful lesson when it successfully referred a case for criminal prosecution, only to result in a bench trial acquittal—after significant investment sunk into the internal investigation that led up to the referral. *United States v. Shiah* thus highlights the importance of careful scrutiny for sufficient evidence of intent by a referring attorney prior to referral. When Tien Shiah left Broadcom to work for fierce competitor Marvell, he gathered up a large number of files and documents he had developed at Broadcom as a "toolkit" of his work. Broadcom apparently went to the Justice Department which charged Shiah with trade secrets theft.

In finding Shiah not guilty after a bench trial, Judge David O. Carter of the Central District of California found that the government had not proven that Shiah intended to convert the trade secrets. See *United States v. Shiah*, 2008 U.S. Dist. Lexis 11973 at *84, *87 (C.D. Cal. Feb. 19, 2008) (finding that "nothing links Shiah's access [of Broadcom files] with nefarious use or any other use of trade secret information" and "there is no evidence demonstrating trade secret information taken from files obtained by Shiah while working at Broadcom and used directly in documents or other work product produced by Shiah while working at Marvell.").

Though Carter noted that Shiah could well face civil liability, he rejected the government's contention that Shiah was criminally liable and rebuked the government for heavily relying on Broadcom's internal investigation. See id. at *79; *90-*92 (noting that more evidence and surveillance would have increased the likelihood of obtaining sufficient probative evidence, but much of the evidence was obtained from Broadcom's investigation rather than the government's; "[w]hen incarceration is at stake, the investigation should be conducted by law enforcement, not law enforcement and a private corporation together.").

The case counsels in favor of scrutinizing a case for sufficient evidence of criminal intent before making a criminal referral. Indeed, it may counsel in favor of exercising patience in tipping the corporate victim's hand about its referral plans and thereby catching the employee in an act that manifests the requisite criminal intent, like making use of the trade secrets. This may ultimately serve the employer better than rushing into a referral after the pilfering employee has merely walked out the door.

Cautionary Tales

But being publicly berated (and losing) after a costly investigation is not the only expense associated with an imprudent criminal referral; the victim company can be on the hook for the ex-employee's legal fees, as well. Such was Goldman Sachs' fate after the acquittal on appeal of ex-employee and accused code pilferer Sergey Aleynikov. When Goldman referred the case to the government, the jurisdictional element as it was stated under the Economic Espionage Act (EEA) at the time required proof that the trade secrets Aleynikov took were "produced for" interstate commerce.

At the trial court level, Aleynikov was convicted of trade secrets theft for taking Goldman Sachs' high-frequency trading system source code to New Jersey and converting it after leaving their employ. But on appeal, he successfully argued that the code was not in interstate commerce, since it was purely internal to the company. *United States v. Aleynikov*, 676 F.3d 71 (2d Cir. 2012). In acknowledging the failure of this criminal prosecution, the U.S. Court of Appeals for the Second Circuit noted that Aleynikov's conduct "was in breach of his confidentiality obligations to Goldman, and was dishonest in ways that would subject him to sanctions; but he could not have known that it would offend this criminal law or this particular sovereign." Id. at 82. Congress later repaired the jurisdictional flaw in the statute, but it was too late for Goldman Sachs, which found itself liable for Aleynikov's legal fees (though Goldman Sachs has appealed the decision to the U.S. Court of Appeals for the Third Circuit). See *Aleynikov v. Goldman Sachs*, 2013 U.S. Dist. Lexis 151603 (D. N.J. Oct. 22, 2013); No. 13-4237 (3d Cir.).

A venue flaw likewise overturned the conviction of Andrew "Weev" Auernheimer, who exploited a security flaw to steal email addresses associated with particular AT&T accounts linked to consumers' iPads. Auernheimer was indicted in New Jersey after revealing what he seemingly believed was a harmless hack to a Gawker reporter. Authorities then charged him with violating the EEA in New Jersey, winning conviction but losing on venue in the Third Circuit on April 11, 2014. See *United States v. Auernheimer*, 2014 U.S. App. Lexis 6671 (3d Cir. April 11, 2014). Given the stakes involved in these trials, certainly it is important not to let the apparent dishonesty or criminality of the defendant's conduct occlude counsel's analysis of all of the elements of the offense.

Unfortunately for the hapless Aleynikov, he has now been charged with the same conduct in New York state court, and a judge recently allowed the prosecution to continue despite the Second Circuit's decision in his federal case. Goldman has also been ordered to advance fees to Aleynikov to defend himself in this state criminal proceeding. While New York has not adopted the Uniform Trade Secrets Act and has no criminal statute specifically addressing trade secrets theft, certain sections of the state criminal code, including the criminal larceny statute, can serve the purpose. Aleynikov, for example, has been charged under N.Y. Penal Law 156.29 (unlawful duplication of computer-related material) and 165.07 (unlawful use of secret scientific material). See also N.Y. Penal Code, Article 155 (Larceny).

Shiah and *Aleynikov* furnish powerful cautionary tales, as does the March 14, 2014 jury acquittal, on all 12 counts, of former Texas Instruments employee Ellen Chen Yeh. See *United States v. Yeh*, 3:08-cr-00096-P (N.D. Tex.). Yeh successfully argued that she lacked the requisite intent to commit or attempt the theft of trade secrets, claiming that she did not

know that copying proprietary information to external storage drives was illegal and that she didn't know that TI's information constituted trade secrets.

Civil Suit

If careful analysis of the evidence reveals a significant flaw in the proof, outside referring counsel should consider recommending a civil suit to the in-house counsel and victim client. As of yet, there is no federal civil statute covering trade secrets misappropriation, and New York has not adopted the Uniform Trade Secrets Act. Rather, in New York, trade secrets are protected by common law.

To establish a claim, the victim must show that (1) it possesses a trade secret, and (2) the defendant has used the trade secret "in breach of an agreement, a confidential relationship, or duty, or as a result of discovery by improper means." See *Hudson Hotels Corp. v. Choice Hotels Int'l,* 995 F.2d 1173, 1176 (2d Cir. 1993) (abrogated on other grounds). Injunctive relief, damages, or both are available, and there is a three-year statute of limitations. Counsel might also consider referral to the state attorney general for civil prosecution under New York's unfair competition law. See NY Code Sec. 2401-2409; Kappos and Baden, "Combating IP Theft Using Unfair Competition Law," NYLJ (May 6, 2013).

Public Relations

Determining that the case is legally sound is only the first step in deciding whether to make the referral. Strategic and public relations considerations abound. As in any criminal referral, the victim company loses control of the case, and while the federal courts have generally been very careful to issue appropriate protective orders, the risk of exposure of trade secrets in the course of the case remains. Further, if the victim company intends to file a civil suit, broader discovery rules could make available non-exculpatory but relevant evidence that the victim would rather keep out of the criminal trial.

The public-relations aspect of criminal investigation and prosecution should not be discounted either. Two recent examples counsel caution. In Washington State, former Microsoft engineer Alex Kibkalo was successfully prosecuted for passing Windows 8 code to a blogger. However, Microsoft's in-house investigation, which included a search of Kibkalo's Hotmail account, exposed the company to adverse media coverage.

And in New York state court, former Two Sigma employee Kang Gao has been subjected to both criminal prosecution and civil suit for taking confidential information with him as he left the hedge fund's employ. In a surprising move, the judge in the civil case publicly called out Two Sigma for referring the case for criminal prosecution, noting that this was the first time he had seen a company have its former employee arrested for a "garden variety" employment dispute. As in *Shiah*, the judge voiced concern over the fact that Two Sigma had investigated the alleged crime, rather than law enforcement. The resulting media portrait of Two Sigma has been less than flattering, particularly considering the startlingly high $1 million price tag on Gao's bail.

Ethical Considerations

Finally, ethical considerations counsel deliberation and care when referring a trade secrets case for criminal prosecution. In their zeal to aid a client, attorneys evaluating referrals can succumb to the temptation to throw whatever they have at the prosecution, perhaps even shading facts—or excluding exculpatory facts—in the process. If the prosecution then goes forward, doesn't that mean that the referral was properly done? But New York State and other ethics rules don't work that way, and neither, potentially, do the results of the prosecution—*Shiah* and *Aleynikov* are key examples.

While criminal referrals are not directly addressed in New York State's rules, its provisions are a reminder that defense attorneys and prosecutors alike have a duty to avoid engaging in conduct involving dishonesty, fraud, deception or misrepresentation and to avoid engaging in conduct that is prejudicial to the administration of justice. See N.Y. Rule of Prof. Resp. 8.4 (c), (d). While it is unclear precisely how such rules would be applied in the context of a conversation between a referring attorney and a prosecutor—for example, does the referring attorney have an obligation to tell the prosecutor evidence that may tend to exculpate the defendant?—as a practical matter, it makes little sense to withhold facts from the prosecutor who may later be sandbagged.

Furthermore, a criminal attorney investigating possible criminal conduct on behalf of a corporate victim client must never use the threat of criminal prosecution against the target to gain an advantage in a civil suit; instead, the attorney must evaluate the case, and make an independent decision whether to refer. See, e.g., N.Y. DR 7-105.

Conclusion

Former employees walk out the door with trade secrets every day. When the facts warrant, victim companies should investigate and refer these individuals for prosecution. But risks must be balanced against potential benefits, because failed prosecutions can harm morale, productivity, and employee retention. A blown-up referral can leave a company looking overbearing by trying to get employees in trouble when they didn't commit a crime. Outside referring counsel well-versed in criminal law have a critical role to play in that judgment call.

Guy Singer *and* ***Mark Mermelstein*** *are partners at Orrick, Herrington & Sutcliffe.* ***Mary Kelly Persyn*** *is an associate at the firm.*
