Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Protecting Trade Secrets Under The EEA

Law360, New York (March 11, 2011) -- The Southern District of New York was recently the scene of two high-profile prosecutions under the Economic Espionage Act of 1996, 18 U.S.C. § 1831 et seq. (the EEA), which, in essence, makes it a federal crime to steal trade secrets.

The two cases — United States v. Samarth Agrawal, 10 CR 417 (JSR), and United States v. Sergey Aleynikov, 10 CR 96 (DLC) — both involved theft of trade secrets relating to proprietary methods of high-speed securities trading, but they offer food for thought for proprietors of trade secrets of any kind.

In both cases, an employee of a financial firm obtained access to computer code used by his employer in its high speed securities trading operation and attempted to take the code to a new employer. Both individuals were prosecuted under the EEA. Both were convicted and await sentencing.

Companies that employ valuable trade secrets in their operations often require employees to sign nondisclosure agreements and/or restrictive covenants that obligate the employee to maintain the confidentiality of the secrets and to refrain from working for competing firms for some period of time after leaving the proprietor's employ.

Ordinarily, breaches of such agreements give rise to civil litigation, with counsel for the former employer rushing to court to seek an injunction enforcing the agreement. As Agrawal and Aleynikov show, the EEA offers an additional avenue for trade secret proprietors to protect their valuable secrets: they can call the U.S. Department of Justice or the FBI.

Invoking the prosecutorial powers of the federal government as a means of protecting trade secrets is a relatively new wrinkle in trade secret law. Taking the Agrawal and Aleynikov cases as examples, this article reviews the background of the EEA and then discusses some of the factors that a trade secret proprietor must consider in deciding whether to seek Uncle Sam's aid in protecting its secrets.

The Statute

The EEA was adopted to provide law enforcement authorities with more effective tools to address theft of intellectual property. The House report on the EEA observed that "there is no federal statute directly addressing economic espionage or which otherwise protects proprietary information in a thorough, systematic manner."

Although transportation of stolen goods across state lines has long been a crime, that provision was "not particularly well suited" to address theft of intangible intellectual property. Id. The EEA was passed "to ensure that the theft of intangible information is prohibited in the same way" as theft of physical goods.

Section 1832 of the act makes it a crime, punishable by fine or imprisonment for up to 10 years, to steal a trade secret for "the economic benefit of anyone other than the owner thereof" while "intending or knowing that the offense will injure any owner of that secret." 18 U.S.C. § 1832(a).

The theft may be accomplished by any of a number of broadly specified means, including not just simply taking the information, but also obtaining it by fraud or deception, copying or replicating it or knowingly purchasing it from another who has stolen it. Attempts and conspiracies are criminalized on the same terms.

The EEA also criminalizes theft of a trade secret while "intending or knowing" that the theft "will benefit any foreign government, foreign instrumentality or foreign agent." 18 U.S.C. § 1831(a). The statute reaches conduct occurring outside the U.S. in certain circumstances. 18 U.S.C. § 1837.

The statute defines the key term "trade secret" to mean "all forms and types of financial, business, scientific, technical, economic or engineering information," provided that "the owner thereof has taken reasonable measures to keep such information secret" and "the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public." 18 U.S.C. § 1839(3).

In addition to criminal penalties, the statute authorizes the attorney general to obtain "appropriate injunctive relief" in a civil action, with federal district courts having exclusive original jurisdiction of such actions. 18 U.S.C. § 1836. However, the EEA does not preempt or displace any other civil or criminal remedies under state or federal law with respect to misappropriation of trade secrets. 18 U.S.C. § 1838.

The EEA thus provides a powerful and potentially very effective weapon against theft of trade secrets. An injunction requiring a former employee to respect a two-year noncompete provision is not nearly as fearsome a sanction as the prospect of spending a similar period in prison.

Moreover, although New York law generally permits enforcement of restrictive covenants, it does so against a public policy backdrop that tends to disfavor such covenants and sometimes limits their enforcement. Contacting the authorities may, therefore, be an attractive option for an aggrieved trade secrets proprietor. There are, however, a number of considerations that the proprietor should keep in mind.

Factors to Consider

Most fundamentally, if the government believes that a theft of trade secrets warrants prosecution, the government will thereafter be in charge of the matter. Although it is in theory possible for a company to pursue civil remedies while the government prosecutes a former employee, in such situations the prosecution will often take priority. Thus, the government may intervene in civil proceedings and seek to stay them.

This consideration did not enter into either Agrawal or Aleynikov, as there were no parallel civil proceedings, but where civil proceedings do exist the government may place them on hold, perhaps for an extended period, while it investigates.

Even without parallel civil litigation, however, the government's control of a criminal prosecution has both potential benefits and potential disadvantages for the trade secret proprietor.

On the advantages side, the government will bear the principal burden of collecting evidence and prosecuting the case, and it has at its disposal very great investigative, forensic and legal resources. The proprietor will find it necessary to cooperate with the government, but it will do so as a crime victim whose rights are being vindicated. It may be subject to some discovery by the defense, but its role will be that of a nonparty witness.

The government's control also has disadvantages, however. Although the trade secret proprietor will have some ability to inform the government's decisions about what specific acts to prosecute, ultimately those decisions rest with prosecutors, not with the victim.

The government may, for example, choose not to prosecute acts that the proprietor will regard as highly injurious, and in particular the government may identify the "trade secrets" in a fashion that is narrower than, or simply different from, the definition preferred by the proprietor.

A related issue is the fact that the trade secret proprietor will not be in charge of methods used to protect the confidentiality of its trade secrets. At trial, the government must prove beyond a reasonable doubt that the defendant took trade secrets. Doing so without disclosing those secrets can be a major challenge.

The EEA permits a court to "enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets," consistent with requirements of the Federal Rules and "all other applicable laws." 18 U.S.C. § 1835. The First and Sixth Amendments are among those laws, however, and they support a strong policy against closing criminal proceedings to the public. Most judges are, therefore, reluctant to do so.

Judges Jed S. Rakoff and Denise L. Cote, who presided over the Agrawal and Aleynikov cases respectively, were not exceptions. Both judges entered protective orders limiting the dissemination of proprietary information before trial, providing, for example, that the defendant was not permitted to view any sensitive information except in the presence of his counsel. Nonetheless, both judges were very reluctant to close any substantial portion of the trial proceedings to the public.

The government, of course, has no interest in compromising the secrecy of trade secrets that it is seeking to defend. The U.S. Attorneys' Bulletin, a bimonthly publication on topics of interest to federal prosecutors, recently carried an article recommending, as a "best practice" in cases under the EEA, that prosecutors "consider minimizing public references to the trade secret" at issue. 57 U.S. Attorneys' Bulletin 2, 15 (Nov. 2009).

This practice was followed in both Agrawal and Aleynikov, with each judge instructing the parties to discuss the secrets at a level of generality such that they would not be revealed in open court. For example, in Aleynikov, testimony revealed that the defendant had accessed certain files, encrypted them, copied them and then deleted his "bash history" in an attempt to cover his tracks, while another witness testified that the files in question contained proprietary trade secret information. All of this testimony was elicited in open court without referring to the contents of the files, i.e., the actual trade secrets at issue.

Nonetheless, it will often be the case that some disclosure of actual trade secrets must be made in order for the government to meet its burden, and in those circumstances there is genuine risk for the trade secret proprietor. The court may not permit the public to be excluded from the courtroom, or may permit exclusion on a narrower basis than the proprietor deems appropriate.

Such concerns are by no means limited to testimonial evidence. Documentary evidence embodying or disclosing trade secrets presents similar risks, particularly when it is common to display such evidence on screens situated around the courtroom.

Finally, even if all of these hazards are successfully negotiated by the trade secret proprietor and its counsel, they must remember that at the conclusion of the criminal proceedings, there will be a group of persons who have, in fact, been given full access to all of the documentary and testimonial evidence in the case: the members of the jury.

Although at the conclusion of the case the jurors will be instructed not to discuss the trade secrets with anyone else (Judges Rakoff and Cote both gave such instructions), there can be no assurance that such an instruction will be scrupulously obeyed, or even remembered, at later times.

For that reason, the trade secret proprietor should attempt to articulate its concerns to prosecutors as fully as possible prior to jury selection, so that in the selection process prosecutors can exercise some vigilance in identifying prospective jurors who, by virtue of their occupation or training, might present a greater risk of misuse or disclosure of trade secrets if exposed to them at trial.

Conclusion

In today's world, trade secrets are more valuable — and more vulnerable — than ever before. The EEA offers an additional means for companies to safeguard their secrets, but also creates a new set of risks and issues for them to consider.

— On Feb. 28, 2011, Judge Rakoff sentenced Samarth Agrawal to three years in prison.

--By Stephen S. Madsen, Cravath, Swaine & Moore LLP
Stephen Madsen is a partner in Cravath's litigation department in the firm's New York office.

The opinions expressed are those of the author and do not necessarily reflect the views of the firm, its clients, or Portfolio Media, publisher of Law360. This article is for general information purposes and is not intended to be and should not be taken as legal advice.