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

What You Should Know About The New Trade Secrets Laws

Law360, New York (February 07, 2013, 3:11 PM ET) -- Congress recently passed two laws that raise the stakes dramatically for employees and anyone else who misappropriates trade secrets. Misappropriation of source code, algorithms or other internally used trade secrets in any industry now may result in criminal convictions, years in jail, and multimillion-dollar fines payable to the U.S. government. Moreover, if the misappropriation benefits a non-U.S. entity, the government now may impose fines well in excess of the previous $10 million cap.

These remedies under criminal law are in addition to other methods that organizations should continue to use to protect their confidential and proprietary information. Those methods include, for example, contractual provisions, internal controls limiting access to information, and civil lawsuits by the firms themselves seeking injunctions and damages.

The first of the two new laws is the Trade Secret Clarification Act of 2012, signed into law on Dec. 28, 2012. It is designed primarily to close the loophole in the Economic Espionage Act that last year caused a federal appeals court to reverse the widely reported conviction of Sergey Aleynikov, a Goldman Sachs Group Inc. computer programmer. Aleynikov had downloaded the source code for Goldman's proprietary high frequency trading platform for potential use by his new employer, a competitor to Goldman. A U.S. district court convicted him for the theft, but an appeals court reversed on the grounds that, among other things, Goldman used the source code only internally and did not sell it. As a result of this new law, the Economic Espionage Act now covers trade secrets related to products and services that an organization develops and uses only internally.

In addition, on Jan. 14, 2013, President Obama signed into law another statute, the Foreign and Economic Espionage Penalty Enhancement Act. This law dramatically increases the maximum fines for organizations and individuals who misappropriate trade secrets of domestic companies in order to benefit a non-U.S. entity.

The Trade Secret Clarification Act of 2012

The Aleynikov Case

While at Goldman Sachs, Aleynikov developed computer source code for Goldman's proprietary high-frequency trading ("HFT") system. He left Goldman to join a start-up company in Chicago that was seeking to develop and implement its own HFT system very quickly. The startup agreed to pay Aleynikov more than double his Goldman compensation to develop the market connectivity and infrastructure components of its new system.

On his last day at Goldman, Aleynikov uploaded to a server in Germany more than 500,000 lines of source code for Goldman's HFT system, including code for a substantial part of the infrastructure and some of the algorithms and market data connectivity programs. At his home in New Jersey that evening, he downloaded the source code from the German server. He subsequently brought the code to meetings at the startup. When he flew home the next day, the FBI arrested him at Newark airport.

A jury subsequently convicted Aleynikov of violating the Economic Espionage Act ("EEA")[1] and the National Stolen Property Act ("NSPA")[2]. He was sentenced to eight years and one month in prison and fined $12,500. The court denied bail, deeming Aleynikov a flight risk. Accordingly, Aleynikov began serving his jail time.

However, one year into his prison term, the United States Court of Appeals for the Second Circuit reversed the conviction.[3] The court found that the EEA did not apply, because Goldman's HFT system was neither "produced for" nor "placed in" interstate or foreign commerce. The court also concluded that the NSPA did not apply to Aleynikov, because the trade secret in question was not tangible property. As a result, Aleynikov was released from jail.

In a concurring opinion, however, Judge Guido Calabresi questioned whether Congress meant to exempt from the EEA the kind of behavior in which Aleynikov engaged. The judge stated that the court had to rule as it did, due to the language set forth in the EEA and the NSPA, but he expressed his "hope" that Congress would amend the statute and "state .. what I believe they meant to make criminal in the EEA."

The Enactment of the Trade Secret Clarification Act

Congress swiftly obliged. Outraged by Aleynikov's acquittal, Congress unanimously passed legislation to broaden the EEA. On Dec. 28, 2012, the president signed into law the Trade Secret Clarification Act of 2012. As a result, the EEA now applies to a trade secret "that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof."

In addition, Aleynikov was re-arrested, this time by the Manhattan District Attorney's Office on state law charges. That prosecution is currently underway.

The Effect of the Trade Secret Clarification Act

With the passage of the Trade Secret Clarification Act, trade secrets protected under the EEA now generally include an organization's internal trade secrets, regardless of whether those secrets are part of something which is sold. There is still a requirement for use in interstate or foreign commerce, but as phrased under the new law, that requirement is now much easier to meet.

In addition, the new law clarifies that services, as well as products, are covered by the EEA.

Unauthorized copying of computer source codes is one type of theft which has led to prosecution, but the EEA broadly covers a wide variety of trade secrets, which includes "all forms and types of financial, business, scientific, technical, economic or engineering information," if the owner has taken reasonable measures to keep the information secret and if the information "derives independent economic value, actual or potential, from not being generally known to or readily ascertainable through proper means by, the public."[4]

The Foreign and Economic Espionage Penalty Enhancement Act

On Jan. 14, 2013, the president signed into law another statute that further broadens the EEA: The Foreign and Economic Espionage Penalty Enhancement Act. This statute increases dramatically the maximum fines for stealing domestic trade secrets in order to benefit a non-U.S. entity.

Under this legislation, the maximum fine for individuals has been raised from $500,000 to $5 million. Moreover, and even more significantly, the maximum fine for organizations is increased from $10 million to the greater of $10 million or "three times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the secret that the organization has thereby avoided."

This new remedy in cases against organizations is important for two reasons.

First, it expressly allows calculation of the fine based on the "value of the stolen trade secret to the organization," which could easily be substantially higher than the $10 million cap that the statute contained prior to the new law. In the Aleynikov case, for instance, the government asserted that the theft cost Goldman $7-$20 million and that it would have taken programmers at least two or three years to write the stolen code from scratch. Accordingly, if Aleynikov had shared the stolen secrets with someone outside of the United States, under the new law he would have been vulnerable to a much higher fine than the $12,500 fine imposed by the trial court.

Second, the new remedy is essentially a punitive damages provision, allowing the government to recover up to three times the value of the stolen trade secret.

The fines under the EEA are payable to the government, not the organization that owns the trade secret.

Deciding Whether to Seek Criminal Prosecution

Internal controls and contractual agreements should remain the primary safeguards used by companies to protect their intellectual property, with civil lawsuits being brought when necessary. However, the two new laws substantially increase the criminal law consequences that a dishonest employee or other thief may face as a result of trade secret misappropriation.

Criminal prosecution of a rogue employee or other wrongdoer can be an extremely attractive prospect from the perspective of the wronged organization. Putting the thief in prison is an excellent way to prevent him from further mischief and to deter others from misappropriation in the first place. Moreover, government prosecutors, unlike private counsel, do not charge for their time. However, there are some important downsides an organization should consider in deciding whether to ask a prosecutor to launch a criminal investigation into the theft of the organization's trade secrets.

Most important, if the government decides to become involved, the organization will cede control of the case to the government. The organization will have no control over the timing or substance of the prosecution itself. The government will determine the misconduct it will focus on, and it may be many months or even years — if at all — before an arrest is made. And, statistically, the government is likely to decline to prosecute.

Moreover, the organization could be forced to halt (or refrain from filing) any civil litigation against the criminal target until the criminal case is finished. This restriction may also apply during the government's investigatory phase, before the prosecutors decide whether to prosecute. Accordingly, for example, involving the prosecutors from the start may mean that the organization will forfeit the opportunity to ask a court to enter an emergency injunction against the former employee and/or the recipient of the information.

So if the organization's primary goal is to immediately prevent a former employee from taking certain actions, such as working for a competitor or servicing particular customers, at the outset, a civil lawsuit may be the organization's best bet, unless the criminal case is unusually compelling or is otherwise attractive to the prosecutors at that time. The organization can, of course, instead consider the prospect of seeking prosecutorial intervention once the initial phase of the civil case is complete.

However, regardless of when the prosecutors get involved, they will follow wherever the evidence leads them, without regard to whether their course serves the interests of the organization. Hence, the prosecutors may decide to pursue a case that is adverse to the organization or that is unrelated to the original problem identified by the organization. Therefore, before approaching the prosecutors, the organization must determine that it is squeaky clean.

Furthermore, particularly if the theft has caused the organization very large financial damages, the organization might prefer to pursue its own civil lawsuit against the former employee and/or the entity receiving the information, instead of asking the government to prosecute. Only the government can sue under the EEA, and any fines imposed under that statute go to the government, not the organization. Moreover, although the prospect of free legal work by the prosecutors is appealing, the organization and its lawyers will still have to do a great deal of work to prepare the case.

Prosecutors are generally inundated with requests to take on cases, and have the luxury of choosing to prosecute only the most attractive cases. To create even a chance of enticing the government to prosecute, the organization and its lawyers will need to prepare the case carefully prior to approaching the prosecutors. And even then, the odds are that the government will decline to prosecute.

Still, as the Aleynikov case shows, there is prosecutorial interest in pursuing trade secret misappropriators in the financial services industry. And the new laws should further embolden federal prosecutors across the country.

Action Items to Protect Proprietary Information

Although the new trade secret laws significantly increase the risks faced by an employee or other person who takes an organization's trade secrets, neither the government nor the organization will succeed in protecting those secrets unless the organization takes appropriate measures to protect them before they are stolen. Without such steps, trade secret status may be lost, thus foreclosing the possibility of a successful civil or criminal lawsuit in the event of a misappropriation.

We recommend consideration of at least the following potential steps:

- Draft or update employment agreements, including confidentiality and noncompete agreements.

- Identify the organization's trade secrets, and then restrict access to them on a need-to-know basis.

- Conduct, and carefully prepare for on a case-by-case basis, exit interviews with departing employees who know or have had access to valuable confidential information of the organization.

- Include confidentiality obligations in the organization's employee manual or code of ethics and require signatures by employees.

- Draft or update confidentiality agreements with third parties such as consultants and vendors.

- Mark as “confidential” documents containing trade secret information.

- Train employees, and then issue periodic reminders to them, about the need for secrecy and their obligation to follow the organization’s rules and practices for protecting confidential information.

- Adopt physical access restrictions such as computer passwords, locked doors and cabinets, building security guards, and electronic sensors on documents.

- Have a computer network-security specialist assess the vulnerabilities of the network and implement a data loss prevention plan.

- Regularly review all of the organization’s advertising, websites, press releases, seminar content and articles to ensure that trade secret information is not disclosed.

An organization need not necessarily take all of those steps, nor is the above list exclusive. An effective plan for the protection of an organization’s trade secrets will be carefully tailored to the needs and practicalities of the particular company. When done right, such a plan will not only lay the groundwork for successful legal action later if it is needed, but more importantly, will maximize the odds that misappropriation will not occur in the first place.

--By Diane Siegel Danoff, Kevin Scanlan and Edward Pittman, Dechert LLP

Diane Danoff is a partner in Dechert's Philadelphia office. Kevin Scanlan is a partner in the firm's New York office. Edward Pittman is counsel in the firm's Washington, D.C., office.

[1] 18 U.S.C. § 1832(a).

[2] 18 U.S.C. §2314.

[3] United States v. Aleynikov, 676 F.3d 71 (2d Cir. 2012).

[4] 18 U.S.C. §1839(3).