HEDGE FUND
legal & compliance digest

www.hedgefundlcd.com May 24, 2016

# New Protections for Trade Secrets Require Fresh Look at Employment Agreements

By Jon Shazar and Jennifer Banzaca

Citadel Investment Group, one of the largest hedge fund firms in the world, is noted for many things, not least its remarkable success. In recent years, however, it has become notable for less vaunted reasons: its inability to keep its trade secrets secret—a series of experiences that have taught it just how varied and uncertain companies' rights and remedies are when an employee absconds with valuable intellectual property.

Indeed, Citadel has been in court almost nonstop since 2009, when it sued a group of former employees it accused of stealing its high-frequency trading code and violating their non-compete agreements with the firm. Citadel won its case against the founders of Teza Technologies, but the remedies afforded them by Illinois law were paltry, at best: The judge in the case refused to extend the former employees' non-compete, and eventually fined their leader just $1.1 million, a drop in the bucket for a man who had earned $150 million in just one year at Citadel.

Stealing trade secrets is, of course, a federal crime: Yihao Pu and Sahil Uppal, two former Citadel employees, pleaded guilty in 2014 to charges—unrelated to the allegations against the Teza founders—alleging theft of the hedge fund's HFT code. But for civil remedies, companies have had to turn to the state courts. And while the case of former Goldman Sachs programmer Sergey Aleynikov, convicted of stealing that bank's HFT code before joining Teza, but cleared by the Second Circuit Court of Appeals, shows that the federal criminal law is itself somewhat fluid, the vagaries of the state courts are even more so: The key jurisdictions of New York and Massachusetts, for example, have not adopted any form of the Uniform Trade Secrets Act.

Now Congress has stepped in to offer some clarity. The Defend Trade Secrets Act, which passed both houses of Congress with just two votes against it, was signed into law by President Barack Obama on May 11. The new law makes theft of trade secrets a federal civil cause of action for the first time, adding it to the other forms of federally-protected intellectual property, copyrights, patents and trademarks. It offers a potential for uniformity that has not existed previously—while also leaving existing state laws in place—and gives aggrieved companies important new recourses if vital proprietary data is misappropriated. As Andy Halaby, a partner at Snell & Wilmer, surmised, "Perhaps the largest impact of the new law is that there is now a federal forum for bringing what otherwise would have been state court civil claims. The federal courts often have more resources than state courts so, in addition to now having a federal law instead of a patchwork of state laws to invoke, you have an entirely different court system which is more resourced and, in some instances, may be better equipped to handle a claim that may require some emergency relief."

Hedge funds and others will have to take a number of affirmative steps in order to take full advantage of the new protections.

The DTSA offers a broad definition of trade secrets, one that encompasses "all forms and types of financial, business, scientific, technical, economic, or engineering information," including plans, formulas, methods, techniques, processes, procedures, programs and codes. That extensive laundry list of both tangible and intangible intellectual property seems likely to prevent the sort of strict reading of the Economic Espionage Act of 1996 that contributed to the Second Circuit's decision to free the former Teza employee, Sergey Aleynikov. (The EEA was amended in 2012 expressly to criminalize Aleynikov's actions.) In order to be covered under the DTSA, firms must take "reasonable measures" to keep the information secret, which information must derive independent economic value from its secrecy.

The trade secret in question must be "related to a product or service used in, or intended for use in, interstate or foreign commerce."

Employees or others misappropriating confidential information meeting the aforementioned standards could be liable for actual damages and unjust enrichment damages, or damages based on a "reasonable royalty." Willful or malicious misappropriation could incur exemplary damages of up to twice the amount of damages initially awarded. What's more, willful or malicious misappropriation could see the defendant hit with attorneys' fees, as could a motion to terminate an injunction made in bad faith. (Opposing such a motion in bad faith could result in the plaintiff facing legal fees, as could claims made in bad faith.)

Arguably the most powerful new weapon given to hedge funds and others seeking to protect their trade secrets is the ability to petition a court for ex parte seizure of a defendant's "property necessary to prevent the propagation or dissemination" of a trade secret. Any application for such a move would require showing irreparable harm and a likelihood of success in proving that the information was obtained "by improper means," and approval would come only in extraordinary circumstances. To ensure that the orders are not abused, firms found to have obtained them in bad faith would face paying a defendant's attorneys' fees—and possibly more.

The DTSA also empowers courts to grant other forms of relief, including injunctions to prevent both actual and threatened misappropriation, requiring affirmative action to protect the trade secrets or, in extraordinary circumstances where such would be "inequitable," the payment of reasonable royalties.

On the issue of ex parte seizure, Halaby added hedge fund managers (indeed, all companies) must meet the stringent requirements of the statute, including demonstrating the defendant is likely to evade the remedies otherwise available as emergency relief; the plaintiff hasn't publicized what the defendant has done; and the plaintiff is prepared to post a bond that gives substantial security in the event the trade secrets alleged stolen are seized, but the court ultimately rules in favor of the defendant.

"There is now another body of law to seek civil remedies against those alleged thieves," Halaby said. "As importantly, they have a new forum, federal court, in which to make those claims. They have an explicit remedy of ex parte seizure of items that contain the alleged trade secrets."

In addition to creating a federal civil right of action, the DTSA also makes several notable changes to the criminal theft of trade secrets law, boosting potential fines from a previous maximum of $5 million to three times the value of the stolen information. It also adds economic espionage and theft of trade secrets to the list of predicate acts qualifying for coverage under the Racketeer Influenced and Corrupt Organizations Act.

Significantly for firms hoping to protect their trade secrets and take advantage of the DTSA's provisions, the new law includes whistleblower immunity provisions which absolve individuals from criminal and civil liability if they provide trade secrets to government officials or disclose them in a document filed under seal in a legal proceeding. Would-be whistleblowers are also allowed to disclose trade secrets confidentially to their attorneys for the same purposes of reporting a suspected theft.

The DTSA mandates that firms comply with strict notice provisions informing employees of the whistleblower protections. In order to seek exemplary damages and legal fees, firms must include language in confidentiality and non-disclosure agreements advising employees and consultants of the law's whistleblower provisions. It further restricts the use of injunctions to prevent someone from entering into an employment relationship, limits restrictions on employment to those based on evidence of threatened misappropriation and prohibits employee non-disclosure agreements from conflicting with state laws barring restrictions on business or trade.

The DTSA has a three-year statute of limitations, beginning when the misappropriation is discovered or should have been discovered.

The DTSA's whistleblower notice provisions take effect immediately, meaning that all other materials dealing with confidential information and intellectual property must be revised to reflect the new requirements. Such notification can be added directly to such agreements, or can be put into a policy document referred to in those agreements.

The adoption of the DTSA comes as the European Union is set to approve its own similar legislation, the Trade Secrets Directive. That law was approved by the European Parliament last month and is set to be finalized by the European Commission. Unlike the U.S. law, which has immediate effect, the Trade Secrets Directive gives EU member states two years to adopt legislation in line with the directive, which aims to harmonize the definition of "trade secret," as well as establish bloc-wide whistleblower protections, much like the DTSA. Unlike the DTSA, however, the directive will not offer EU-wide uniformity, as individual countries have some latitude in matters such as employee mobility and statutes of limitations. What's more, there would be no exemplary damages under the EU directive.