Connecticut Law Tribune

Taking Steps To Fight Trade Secret Misappropriation

CONGRESS PASSES TWO LAWS TO STRENGTHEN THE ECONOMIC ESPIONAGE ACT
By PATRICIA REILLY and MATTHEW CURTIN

January 25, 2013

Congress recently passed two separate bills aimed at strengthening the Economic Espionage Act of 1996 (EEA) and deterring trade secret misappropriation. These important changes to the EEA are intended to reverse the highly criticized decision in United States v. Aleynikov, 676 F.3d 71 (2d Cir. 2012), and address increased theft of corporate trade secrets to benefit foreign entities.

The first bill, the Theft of Trade Secrets Clarification Act of 2012, broadens the scope of trade secret protection under the EEA. The second bill, the Foreign and Economic Espionage Penalty Enhancement Act of 2012, enhances the criminal penalties available pursuant to a conviction concerning economic espionage as defined by the EEA.

Economic Espionage Act
The EEA, 18 U.S.C. §§1831-1839, was the first federal law specifically addressing trade secret misappropriation. The EEA is a broad criminal statute allowing for substantial penalties, including millions of dollars in fines, imprisonment, and property forfeiture.

The EEA protects against two specific types of criminal offenses: (1) theft of trade secrets under 18 U.S.C. §1832; and (2) economic espionage 18 U.S.C. §1831, i.e., theft of trade secrets with the added element that the individual committing the offense knew that the offense would benefit a foreign government, foreign instrumentality, or foreign agent.

United States v. Aleynikov
In Aleynikov, the defendant was a former Goldman Sachs computer programmer employee who helped develop the investment banking firm's source code for its proprietary high-frequency trading (HFT) system. The HFT system is the investment firm's proprietary internal system for securities and commodities trading that executes large volume trades within fractions of a second.

The programmer decided to leave the investment firm and join a startup company for nearly triple the salary he was making at Goldman Sachs. On his final day of employment with the investment firm, the programmer uploaded to a server in Germany approximately 500,000 lines of the HFT's source code for use in his new employment. His new employer sought to create its own HFT system apparently using Goldman Sach's source code. The programmer was caught, arrested by the FBI, and convicted of violating the EEA.

But the U.S. Court of Appeals for the Second Circuit overturned his conviction. In doing so, the Second Circuit narrowly construed Section 1832 of the EEA, pointing out that a trade secret must be "related to or included in a product that is produced for or placed in interstate or foreign commerce."

The Second Circuit concluded that the Goldman Sachs HFT system was neither "produced for" nor "placed in" interstate or foreign commerce because it had no intention of selling its HFT system or licensing it to anyone. Simply put, because the firm's HFT system was meant for internal use, the source code was not a "trade secret" covered by the EEA.

Seemingly recognizing the injustice of the Second Circuit's reversal of the programmer's conviction under the EEA, Judge Guido Calabresi cautioned in a concurring opinion that the programmer's actions were precisely the type of "mischief" that the EEA aims to prohibit and invited Congress to "return to the issue and state, in appropriate language, what I believe they meant to make criminal in the EEA."

Enhancing The EEA

Heeding Judge Calabresi's invitation, Congress immediately took up legislation to close the loophole. Congress also sought to strengthen the EEA's penalties to deter increased misappropriation of corporate trade secrets, particularly misappropriation benefitting foreign entities. Congress approved two bills, one broadening the scope of trade secrets covered under the EEA and the other enhancing the criminal penalties available for economic espionage offenses under the EEA.

The first bill, the Theft of Trade Secrets Clarification Act of 2012, is an explicit rejection of the Second Circuit's decision in Aleynikov. As discussed above, prior to the Clarification Act, Section 1832(a) of the EEA required that a trade secret be "related to or included in a product that is produced for or placed in interstate of foreign commerce . . . ." Practically speaking, as evidenced by the Aleynikov decision, this language protected only trade secret information concerning products an entity sells as opposed to products an entity uses internally, like Goldman Sachs' internal source code.

The Clarification Act amends Section 1832(a) of the EEA so that a trade secret must now be "related to a product or service used in or intended for use in interstate or foreign commerce . . . ." This amendment will broaden the EEA so that it now covers not only trade secrets related to products a company sells or intends to sell, but internal products such as the source code.

On January 1, 2013, Congress also passed the Foreign and Economic Espionage Penalty Enhancement Act of 2012. The act aims to strengthen the EEA by enhancing available criminal penalties for an "economic espionage" offense under Section 1831 of the EEA.

The Penalty Enhancement Act increases maximum fines for individuals and organizations convicted of an "economic espionage" offense. Under the current version of the EEA, an individual convicted of economic espionage may be fined up to $500,000 and imprisoned up to 15 years, while an organization convicted of a similar offense may be fined up to $10 million.

The Penalty Enhancement Act also increases the maximum fine for an individual from $500,000 to $5 million. The maximum fine for an organization will increase from $10 million to the greater of $10 million or three times the value of the stolen trade secrets.

In addition to increased monetary penalties, the Penalty Enhancement Act instructs the United States Sentencing Commission to "review and, if appropriate, amend the Federal sentencing guidelines" concerning convictions for economic espionage with the intent to benefit a foreign entity.

Conclusion

That a lame-duck Congress was able to pass two separate bills significantly amending the EEA, all while attempting to deal with the ubiquitous "fiscal cliff," speaks to the increasing importance of trade secret misappropriation and economic espionage.

It's possible that the enhancements to the EEA also could be a first step towards Congress providing corporate entities a civil cause of action for trade secret misappropriation. With some circuit courts restricting the use of the Computer Fraud and Abuse Act as grounds to pursue former employees for trade secret misappropriation, a federal civil cause of action that would allow corporate entities to sue former employees for trade secret misappropriation would surely provide another useful tool for businesses to protect their legitimate interests in proprietary information..

In any event, the broader EEA will likely spur an increased effort to federally prosecute trade secret theft and protect domestic business interests from corporate espionage. •

Patricia Reilly is a shareholder in the New Haven office of Littler Mendelson. She represents clients in a range of employment law matters, with an emphasis on the litigation of employment discrimination and related torts; wage and hour issues; and trade secrets and unfair trade practices disputes. Mathew Curtin is an associate in the firm's New Haven office.