Client Alert

pillsbury

Litigation

February 11, 2013

Congress Raises the Stakes for Theft of Trade Secrets with Passage of Two New Laws

By Kenneth W. Taber and Ranah L. Esmaili

The old adage that crime does not pay rings particularly true in the aftermath of two pieces of recent legislation aimed at raising the penalties for trade secret theft: the Theft of Trade Secrets Clarification Act and the Foreign and Economic Espionage Penalty Enhancement Act.

The United States government has become increasingly focused on the monetary costs to the economy from the theft of trade secrets – costs that can never be fully known, but have been estimated to run into the hundreds of billions of dollars. While the Department of Justice and FBI have stepped up prosecutions of individuals and corporations engaging in such theft under the Economic Espionage Act of 1996 (the "EEA"), a recent Second Circuit decision, *United States v. Aleynikov*, 676 F.3d 71 (2d Cir. 2012), exposed significant limitations in the reach of the EEA – punishing the theft of trade secrets incorporated in products placed in interstate commerce, but not if these products are only used to facilitate or engage in commerce. Certain intangible intellectual property and services were therefore not protected under the EEA – a significant limitation, considering the increasing technology and service orientation of the economy.

Congress has now reacted promptly, passing legislation to close these gaps, and to substantially increase the penalties associated with trade secret theft for the benefit of foreign governments. While the EEA still does not provide a private right of action, the likely result of these legislative initiatives will be an increase in the number of criminal referrals and enforcement actions.

The Economic Espionage Act of 1996

The EEA, 18 U.S.C. § 1831, *et seq*., punishes companies and individuals who (i) knowingly misappropriate a trade secret (defined broadly as financial, business, scientific, technical, economic or engineering information) "that is related to or included in a product that is produced for or placed in interstate or foreign commerce," to the economic benefit of anyone other than the owner, (ii) misappropriate a trade secret knowing that it will benefit a foreign government, or (iii) attempt or conspire to commit such theft. As under common law, the EEA requires the owner to have taken reasonable measures to keep such information secret, and that the information derive economic value from not being known to, or ascertainable by, the public.

The EEA carried the threat of maximum penalties of $250,000 and ten years imprisonment for individuals, and maximum penalties of $5,000,000 for organizations. Where the theft was for the benefit of foreign governments, the maximum penalties doubled and the maximum imprisonment for individuals increased to fifteen years. The EEA also allows the Attorney General to bring a civil action to obtain injunctive relief against violations of the EEA.

The Second Circuit Limits the Scope of the EEA

What the EEA did not reach was brought into sharp focus by *Aleynikov*. In 2009, a former Goldman Sachs Group Inc. ("Goldman") programmer was indicted for stealing Goldman's proprietary source code for its high-frequency trading program upon his departure for a Chicago-based startup looking to develop its own such program. *Aleynikov*, 676 F.3d at 73. On the defendant's last day with the company, he encrypted and uploaded more than 500,000 lines of Goldman source code to a server in Germany, then deleted the encryption program and history on his computer. *Id.* at 74. He then downloaded the source code from that server in Germany to his home computer and took portions on a flash drive to a meeting in Chicago with the startup. *Id.* The jury convicted the defendant and he was sentenced to 97 months of imprisonment and ordered to pay a $12,500 fine. *Id.* at 75.

The defendant appealed, arguing that the stolen source code was not "related to or included in a product that is produced for or placed in interstate or foreign commerce," within the meaning of the EEA. *Id.* The Second Circuit agreed, reading this statutory language to apply only to products that have "already been introduced into the stream of commerce and have reached the marketplace," and products that are "still being developed or readied for the marketplace." *Id.* at 80. The Court said the statute did not apply where a product's purpose is merely to facilitate or engage in such commerce. *Id.* It therefore reversed the defendant's conviction.

The Legislative Fix

Congress reacted swiftly to this decision, passing the Theft of Trade Secrets Clarification Act of 2012, signed into law on December 28, 2012. As Senator Patrick Leahy (D-VT) explained, this act was aimed at correcting the Second Circuit's "narrow reading" of the EEA to ensure that "American companies can protect the products they work so hard to develop, so they may continue to grow and thrive." The law replaced the statutory language the Second Circuit had narrowly construed, "a product that is produced for or placed in interstate or foreign commerce," with the phrase "a product ***or service used in*** or intended for use in interstate or foreign commerce." (emphasis added.)

Congress then followed with the Foreign and Economic Espionage Penalty Enhancement Act of 2012, signed into law on January 14, 2013, increasing the maximum penalties for trade secret theft by those who knowingly commit economic espionage to benefit a non-U.S. government, agency or instrumentality. The stated purpose of this bill was to protect U.S. jobs and technologies, promote investments and innovation, and advance the economic and national security interests of the United States. The maximum penalties for such foreign economic espionage by individuals increased from $500,000 to $5,000,000. For organizations, the penalties increased from $10,000,000 to "the greater of $10,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided." The new law also charges the United States Sentencing Commission with evaluating and, if appropriate, amending the federal sentencing guidelines for foreign trade secret theft convictions. Notably, the act did not increase the maximum penalties, or mandate sentencing guideline review, for purely domestic thefts.

Conclusion

Enforcement officials now have the authority to commence criminal and civil proceedings against individuals and organizations who steal trade secrets related to services, and products or services used to facilitate interstate or foreign commerce. These recent legislative changes will criminalize the theft of more types of intangible intellectual property and afford greater protection, in particular, to the financial services industry. Moreover, recognizing that economic espionage is all about monetary gain, the changes will better align the penalties for such wrongdoing with the potentially enormous benefits to be reaped by offenders, at least in the context of thefts for the benefit of foreign governments and instrumentalities.

If you have any questions about the content of this alert, please contact the Pillsbury attorney with whom you regularly work, or the authors below.

Kenneth W. Taber (bio)
New York
+1.212.858.1813
kenneth.taber@pillsburylaw.com

Ranah L. Esmaili (bio)
New York
+1.212.858.1526
ranah.esmaili@pillsburylaw.com

This publication is issued periodically to keep Pillsbury Winthrop Shaw Pittman LLP clients and other interested parties informed of current legal developments that may affect or otherwise be of interest to them. The comments contained herein do not constitute legal opinion and should not be regarded as a substitute for legal advice.
© 2013 Pillsbury Winthrop Shaw Pittman LLP. All Rights Reserved.