SEYFARTH SHAW LLP
ATTORNEYS

2029 Century Park East, Suite 3500
Los Angeles, California 90067-3021
(310) 277-7200
fax (310) 201-5219
www.seyfarth.com

Writer's direct phone
(310) 201-1579

Writer's e-mail
rmilligan@seyfarth.com

April 22, 2013

Docket No: IPEC-2013-XXX

Re: Trade Secret Theft Strategy Legislative Review

I am submitting this letter in my personal capacity in response to the request by the U.S. Intellectual Property Enforcement Coordinator (IPEC) for public input to determine if there are legislative changes that would enhance enforcement against, or reduce the risk of, the misappropriation of trade secrets for the benefit of foreign competitors or foreign governments.

My practice focuses on trade secret, non-compete, and data protection litigation and transactional work on a state, national, and international platform and my comments are based upon my experience litigating and counseling clients on trade secret and other intellectual property issues.

The threat to U.S. companies' trade secrets is well documented in the Obama Administration's Strategy on Mitigating the Theft of U.S. Trade Secrets, the Department of Justice's Department of Justice's "Summary of the Major U.S. Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases", as well as recent studies by Mandiant, CREATE.org., and Symantec, as discussed below.

While the risk of the continued misappropriation of trade secrets by or for the benefit of foreign competitors or foreign governments is real, the present legal system does not provide adequate protection to U.S. companies for international trade secret misappropriation. A federal civil claim may provide an effective mechanism to deter such theft and provide an effective remedy against such theft.

I played a leading role with the American Bar Association Section of Intellectual Property Law's recent passage of a resolution supporting a federal civil claim for the misappropriation of a trade secret when certain circumstances are present and certain specified requirements are met.

The resolution provides for the expanded federal jurisdiction for civil actions for misappropriation of trade secret claims incorporating five general principles:

- A definition of trade secrets that is comprehensible and expansive versus restrictive and overly technical;

- The availability of remedies that are similar to the Uniform Trade Secrets Act ("UTSA"), including injunctive relief, royalty damages, attorneys' fees, and exemplary damages;

- A comprehensible definition of what requirements must be met to trigger exclusive federal jurisdiction, which includes, at a minimum, claims involving the theft of trade secrets by or for the benefit of foreign governments, companies, or individuals;

- A seizure order provision that adequately addresses how seized information should be stored or protected, who will gather it, and who will have access to it; and

- A provision addressing the interplay between state trade secret claims brought under the Uniform Trade Secrets Act adopted by the vast majority of states and common law claims when an action is brought under the proposed legislation which does not interfere with the pursuit of those claims under applicable state law.

The enclosed Resolution provides more specific details concerning the general framework as well as some of the reasons why a federal civil cause of action for trade secrets theft is needed. I have outlined some of those reasons below:

- Published reports indicate that there is a growing rise in trade secret theft from foreign hackers and rogue employees interested in obtaining U.S. businesses' trade secrets. Foreign economic collection and industrial espionage against the United States represent significant and growing threats to the nation's prosperity and security. The Obama Administration's recently released report regarding trade secret theft recognized the accelerating pace of economic espionage and trade secret theft against U.S. corporations. For example, it provides the example of a recent case where a project engineer for a large car manufacturer copied 4,000 documents onto an external hard drive and delivered them to a competitor in China. The documents contained trade secret design specifications for engines and electric power supply systems estimated to be worth between $50 million and $100 million. Further, the Justice Department's recent challenges in serving foreign defendants in the Kolon criminal action demonstrate some of the present inadequacies in federal law.

Additionally, a respected security company recently published a report finding that foreign governments are sponsoring cyber-espionage to attack top U.S. companies. Further, a recent report commissioned by a respected IT security company revealed that half of the survey respondents, employees from various countries, including the United States, indicated that they have taken their former employer's trade secret information, and 40 percent say they will use it in their new jobs, and one its other reports indicates that cybercriminals are targeting the intellectual property of U.S. companies, particularly small businesses.

- The recent expansion of penalties and expanded definition of trade secret under the Economic Espionage Act reflect a recognition by the government that the Act is a valuable tool to

protect secret, valuable commercial information from theft and that Congress can work in a bipartisan effort to address such theft.

- The United States currently has an un-harmonized patchwork of trade secret protection laws that are ill-equipped to provide an effective civil remedy for companies whose trade secrets are stolen by or for the benefit of foreign governments, companies, or individuals. Not all states have adopted the Uniform Trade Secret Act, and many differ in the interpretation and implementation of certain trade secret laws. Moreover, victims of trade secret theft often face lengthy and costly procedural obstacles in obtaining evidence when the misappropriators flee to other states or countries or transfer the evidence to other states or countries. Additionally, the Department of Justice has limited resources to pursue international criminal trade secret misappropriation claims. A federal civil claim for trade secret misappropriation involving international trade secret theft, including necessary extraterritorial language, will provide the private sector with a viable mechanism and remedies to protect their trade secrets from foreign interests.

Accordingly, I believe the IPEC should support United States Senator Christopher Coons' recent efforts to create a federal civil claim for the misappropriation of a trade secret consistent with framework outlined in this letter and the enclosed Resolution.

Lastly, to further protect the nation's valuable trade secrets and security, I believe that IPEC should consider 1) proposing clarifying that the Computer Fraud and Abuse Act applies to employee data theft; 2) enhancing the penalties for violations of the Economic Espionage Act; 3) providing U.S. Customs with greater clarity concerning its ability to seize products containing misappropriated trade secrets; and 4) clarifying the service requirements in Economic Espionage Actions brought against foreign actors to ensure the extraterritorial reach of United States law.

If I can provide any further assistance or information, please do not hesitate to let me know.

Very truly yours,

/s/ Robert B. Milligan

RBM:jh
Enclosures