A Tool For Fighting Economic Espionage

By DAVID S. POPPICK

The Economic Espionage Act ("EEA"), 18 U.S.C. §§ 1831-39, gives companies another tool in the fight against misappropriation of trade secrets to "adopt a national scheme to protect U.S. proprietary economic information" and to combat the rising tide of espionage against and threats to corporate trade secrets. It criminalizes misappropriation of trade secrets.

The EEA creates a crime for the misappropriation of a trade secret to the economic benefit of anyone other than the trade secret owner generally, or specifically a foreign government. For example, in June 2008, a former Chinese national who admitted he tried to sell fighter pilot training software to the Chinese navy was sentenced to two years in prison. See United States v. Meng, No. 04-CR-20216, slip. op. (N.D. Cal. June 18, 2008). The EEA also prohibits "attempts" and "conspiracies" to commit economic espionage.

The standard definitions of trade secrets apply, as do the rules that the owner must have taken measures to keep the information secret, and the information must derive independent economic value from not being known and not being readily ascertained through proper means.

The penalties that may be imposed under the EEA are severe. An individual convicted of theft of a trade secret under this statute for economic espionage with a foreign government, instrumentality or agent faces a maximum sentence of 15 years in prison and/or a fine up to $500,000. A corporation or other organization held in violation of foreign espionage is subject to a maximum fine of $10 million. In cases of trade secret conversion in interstate or foreign commerce for economic benefit, a person faces a fine and/or 10 years in prison, and a corporation can be fined up to $5 million.

Special Features

The EEA requires the court to enter orders to preserve the confidentiality of the trade secret in any proceeding under the act. Without that, the owner of a trade secret may be reluctant to cooperate in an EEA prosecution for fear of exposing the trade secret to public view.

Additionally, the EEA provides for criminal forfeiture of "any property constituting, or derived from, any proceeds the person obtained, directly or indirectly," from the theft of the trade secret. Additionally, "any of the person[s] property used . . . to commit or facilitate the commission [of the offense]" may also be forfeited. Although the property is forfeited to the United States, the victim should seek restitution from the proceeds of the forfeiture.

If a party resides in the United States, but commits the act of espionage in a foreign country, that act of espionage is subject to the EEA. Also, if a foreign corporation sells a product containing a trade secret in the United States, it may be prosecuted under the EEA as long as the misappropriation occurred in the United States.

The trade secret owner must weigh the benefits and risks of a prosecution before requesting the government to commence a case. For example, a prosecution shows competitors that the owner of the trade secret is serious about protecting its proprietary and confidential information. Conversely, in an EEA prosecution, the owner of the trade secret loses control of the case to the government, which may not have the same interests. Additionally, the criminal defendant may be entitled to production of the trade secret as part of discovery, subject to a court protective order preserving confidentiality.

Because the trade secret owner relies on the U.S. attorney’s office’s willingness to prosecute, it is important to consider the questions that the government may ask in deciding whether to commence a case under the EEA. First, what was the adequacy of the security measures? Second, what kind of information was misappropriated? It is likely that the government will be more interested in pursuing a case involving scientific or research information because it may have longer lasting value. (A marketing plan may have no value by the time a case proceeds to trial.)

Third, is there hard evidence of misappropriation, particularly physical evidence or admissions? Fourth, is the trade secret owner willing to cooperate fully with the government? Fifth, does the defendant have a strong defense to the action? Sixth, what is the timing of the referral? In some cases, it may be better to report the theft imme-
diately, while in other instances it may be wise to conduct a full, private investigation before contacting the U.S. attorney’s office. Seventh, does the trade secret have value and can it be documented? Finally, does the victim have the resources to pursue a civil remedy?

**Defenses**

A defendant to an action brought under the EEA has the three traditional defenses used in trade secret actions: (1) independent parallel development of the trade secret; (2) reverse engineering; and (3) general knowledge, skills or experience. See *United States v. Hsu*, 155 F.3d 189, 196-97 (3d Cir. 1998).

**Representative Cases**

In *United States v. Lange*, 312 F.3d 263 (7th Cir. 2002), the defendant’s conviction under the EEA was upheld over his denial that the computer data he stole from his former employer and attempted to sell to a competitor met the statutory definition of “trade secret.” The court held that the former employer took reasonable measures to keep the computer data secret, including storing all of the data in a room protected by a special lock, alarm system, motion detector; keeping the number of copies and employees’ access thereto limited; and dividing its work among several vendors to ensure that no vendor could replicate the product. See also *United States v. Four Pillars Enterprise Co.*, No. 06-3297, 2007 WL 3244034 (6th Cir. Oct. 30, 2007) (The defendant was convicted of attempt and conspiracy to commit theft of trade secrets in violation of the EEA for scheme to obtain confidential and proprietary information from employer).