Westlaw Journal
INTELLECTUAL PROPERTY
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 19, ISSUE 1 / MAY 3, 2012

Expert Analysis

Four Lessons Every Company Needs to Know About Protecting its Trade Secrets

By Peter J. Toren, Esq.
Weisbrod Matteis & Copley

The Economic Espionage Act was enacted 16 years ago to great fanfare and with the goal of better protecting critical U.S. corporate information from theft by foreign governments and unscrupulous competitors. In signing the EEA, President Bill Clinton stated, "The act establishes a comprehensive and systematic approach to trade-secret theft and economic espionage."[1]

After a relatively slow start largely due to the commitment to fight terrorism after 9/11, the government in the past four years has begun devoting more resources to investigating and prosecuting cases involving the theft of trade secrets. In the middle of 2010 the FBI and the Justice Department announced they had recently opened 66 investigations of theft of trade secrets and economic espionage under the EEA.[2]

Shortly thereafter, the Justice Department announced an increase in the number of EEA prosecutions and promised to make them a high priority for law enforcement.[3] In fiscal year 2011, as compared with fiscal year 2010, the Justice Department and the FBI saw an increase of 29 percent in investigations of economic espionage and theft of trade secrets.[4]

Even with the increased pace of prosecutions in recent years, however, the government so far has brought only about 115 prosecutions under the two separate provisions of the EEA. Breaking it down further, the government has brought nine cases under 18 U.S.C. § 1831, which requires the government to prove the theft was intended to benefit a foreign government, instrumentality or agent.

The remainder of the prosecutions were brought under Section 1832, which is a general criminal trade-secrets statute. Despite its inclusion in the EEA, there is no requirement of foreign espionage in this provision. Rather, Section 1832 applies to anyone who knowingly engages in any act of misappropriation "with intent to convert a trade secret, 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 thereof, and intending or knowing that the offense will injure any owner of that trade secret."[5]

In other words, Section 1832 is intended to be a law of general applicability.

The United States has now brought a sufficient number of prosecutions under the EEA that we are able to draw meaningful conclusions from a review and analysis of them. Indeed, such an examination reveals a number of expected and unexpected results that corporations should strongly consider in implementing or improving upon a trade-secret-protection program.

A review of the prosecutions that the United States has brought under the EEA since it was enacted in 1996 points to at least four things that companies should know to help them better protect their trade secrets.

LESSON #1: IT'S USUALLY AN INSIDE JOB

First, in more than 90 percent of the EEA prosecutions, the defendant was an "insider" and had access to the trade secrets because he or she either was an employee of the victim or worked for a vendor or contractor of the victim. Companies should be aware that defendants almost always misappropriate the trade secrets shortly before resigning from the victim company.

This means when an employee who has access to confidential information informs a company that he or she is leaving, the company should not only immediately revoke the employee's ability to access all proprietary information, but also consider whether to launch an investigation into the employee's computer records over the previous few months to see whether there is any suspicious activity.

At the very least, a company should conduct an exit interview with the employee and require him or her to attest that he or she is not taking any confidential or proprietary information to a new employer.

The risk to companies posed by employees stealing trade secrets shortly before departing cannot be understated. For example, an Intel Corp. engineer agreed April 5 to plead guilty to stealing more than $1 billion in trade secrets just before he left to begin work at rival Advanced Micro Devices. *United States v. Pani*, No. 4:08-CR-40034 (D. Mass. 2008).

According to the indictment, the trade secrets included details on the development of Intel's newest generation of microprocessors. The defendant intended to use the information to further his career at AMD.

LESSON #2: 'THE CHINA CONNECTION'

Second, companies should be aware that the threat posed by foreign economic espionage is real, and the risk is increasing. In particular, there is a "China connection" in a strikingly high percentage of the prosecutions. In more than 20 percent of these cases, the defendant misappropriated trade secrets to benefit the Chinese government or an existing Chinese company or to start a company there.

This trend is increasing. Before 2006 there were very few prosecutions with a China connection, but by 2010, six of the seven cases adjudicated under the EEA involved a link to China. This emerging trend confirms an understanding that, as part of the country's development process, China's intelligence services, as well as private companies and other entities, frequently seek to exploit Chinese citizens or people with family ties to China who can use their insider access to U.S. corporations to steal trade secrets with the use of a variety of methods.[6]

For example, a former engineer at Ford Motor Co. was sentenced to 70 months' imprisonment April 12, 2011, for stealing trade secrets shortly before he left the

company in 2007 to work for a competitor in China. When the defendant returned to the United States on a business trip in 2009, the FBI arrested him and discovered that 41 Ford system-design specification documents had been downloaded onto his laptop computer that belonged to his new employer, Beijing Automotive Co., and the documents had been accessed while he was employed there. *United States v. Yu*, No. 2:2009-CR-20304 (E.D. Mich.).

LESSON #3: JUST BECAUSE YOU DON'T LIVE IN SILICON VALLEY DOESN'T MEAN YOU'RE EXEMPT

Third, although many of the prosecutions involved sophisticated technology, there was no shortage of cases involving other types of trade secrets. In about 15 of the cases, the trade secrets comprised computer source code and algorithms relating to a variety of products and systems. Six of these cases involved source code used by financial services firms.

For example, the U.S. attorney's office for the Northern District of Illinois obtained an indictment Sept. 28, 2011, against Chunlai Yang for stealing trade secrets from CME Group. *United States v. Yang*, No. 1:2011-CR-00458 (N.D. Ill.).

According to the indictment, Yang, who began working for CME in 2008, misappropriated software programs that supported the company's Globex electronic trading program, which allowed market participants to buy and sell exchange products from any place at any time.

The source code in other cases was related to technology used in the processing of health forms; platforms for location-based services; applications for mobile phones, Windows NT and Windows 2000; and designs for computer chips.

In addition to the theft of source code, about five cases related to computer hardware or machines used to manufacture computer chips. For example, a defendant pleaded guilty to downloading 8,800 files from KLA-Tencor's computer network containing trade secrets related to a wafer-inspection tool. This tool used highly magnified light optics and sophisticated algorithms to detect flaws on silicon wafers being manufactured into processors and memory chips. *United States v. Murphy*, No. 5:11-CR-00029 (N.D. Cal.).

The trade secrets in about seven of the cases related to formulas for new drugs or to medical devices in general. For example, Yuan Li, a former Sanofi Aventis employee and Chinese national, pleaded guilty to misappropriating a number of Sanofi's proprietary and secret drug compounds, including their chemical structures, and offering to sell them through the website of a Chinese company. *United States v. Li,* No. 2:2012-CR-00034 (D.N.J. 2011).

In a case involving medical devices, a former scientist at Roche Diagnostics pleaded guilty to stealing trade secrets for a hepatitis monitoring kit he hoped to sell in China. *United States v. Pei,* No. 98-CR-4090 (D.N.J.).

Other recent subject areas of interest to thieves of trade secrets include automobile designs, solar cells, foam insulation and fireproofing technology. In addition to high-tech trade-secret information, cases have also involved the theft of maintenance manuals, information related to smokeless tobacco products, sales information and internal pricing information. The bottom line is that no type of proprietary information should be considered immune from theft so long as the information has economic value to a third party.

LESSON #4: CHANCES ARE YOUR SAFEGUARDS AREN'T AS SAFE AS YOU THINK

Fourth, a number of cases suggests that regardless of the steps undertaken by a company to protect trade secrets, the protection is only as strong as the weakest link. In one case, the victim company undertook more than reasonable measures to protect its trade secrets. Its physical security measures included carefully controlled access to the company's facilities, security cameras at the entrances to the buildings and a large security force.

The company's network and computer security included passwords and firewalls to prevent infiltration by hackers and other outside threats. The company also had measures in place to protect confidential and proprietary information internally, including restricting access within the company's network depending on the user's authorization and the classification status of a document or file. It had a specific trade-secret protection program that detailed policies regarding the classification and marking of proprietary documents and access to documents and their physical handling. This program provided for the training of new hires and current employees, as well as audits to promote compliance with the program's policies.

The company required its employees to sign an employment agreement, a code of conduct containing a confidentiality provision and a policy on the appropriate use of computer resources. Upon hiring, the company informed employees of its policy regarding the protection of proprietary information, including classification levels, and employees were reminded of their obligation to maintain the secrecy of the company's proprietary information through regular training and audits.

Despite this multi-pronged approach, a company software engineer was able to download thousands of company documents onto her personal laptop and a thumb drive, and very few of the documents related to her work. She was also able to leave the company premises on a number of occasions carrying documents in her arms, even late at night. She accomplished all of this on her first day back at work after a more than one-year absence for medical reasons.

Instead of restricting her access to the computer network, the company apparently gave her authority to access many documents that did not relate to her work. Also, the record apparently does not contain evidence that the company sought to learn what she had been doing during her leave of absence. Had the company done so, it might have learned that she had traveled to China and agreed to go to work for a competitor there.

The defendant probably would have succeeded had she not been stopped at a Chicago airport as she attempted to board a flight to Beijing. She was only detained and searched after she had given misleading answers to a customs officer about how much cash she was carrying. If this had not occurred, the company may never have learned about the thefts or, at the very least, the defendant would have been able to return to China with all the company's documents. *United States v. Jin,* No. 08-CR-192 (N.D. Ill.).

Although the government has stepped up its investigations and prosecutions for theft of trade secrets, companies should not and cannot rely on the government for protection. Corporate victims should report thefts to the government because criminal prosecutions can serve to deter future thefts. However, companies should

seriously evaluate their intellectual property protection programs to determine whether they are doing everything possible to prevent thefts.

Legal experts should be included in this process to make sure that the company is not running afoul of any laws and is protecting its valuable information in a manner that preserves all available legal protections. Given the findings of a survey of the EEA prosecutions to date, the review should emphasize internal threats and the danger of foreign economic espionage, especially to high-tech companies. Companies should stay informed of legal and security developments in this area to be able to adjust their protection programs as warranted.

NOTES

1 Statement by President Bill J. Clinton upon signing H.R. 2723, reprinted in 1996 U.S.C.C.A.N. 4034.

2 Press Release, Dep't of Justice, Department of Justice Joins in Launch of Administration's Strategic Plan on Intellectual Property Enforcement as Part of Ongoing IP Initiative (June 22, 2010), *available at* http://www.justice.gov/opa/pr/2010/June10-ag-722.html.

3 2010 U.S. Intellectual Property Enforcement Coordinator Annual Report on Intellectual Property Enforcement, at 4 (February 2011), *available at* http://www.cybercrime.gov/ipecreport2010.pdf.

4 2011 U.S. Intellectual Property Enforcement Coordinator Annual Report on Intellectual Property Enforcement, at 30 (March 2012), *available at* http://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_annual_report_mar2012.pdf.

5 18 U.S.C. § 1832(a).

6 2011 U.S. Intellectual Property Enforcement Coordinator Annual Report, at 30.

Peter J. Toren is a partner with **Weisbrod Matteis & Copley** in Washington. Previously, he was a partner with Sidley Austin in New York and a federal prosecutor in the Justice Department's Computer Crime and Intellectual Property Section, where he served as lead prosecutor in a number of high-profile cases involving the Economic Espionage Act, Computer Fraud and Abuse Act, and copyright and trademark violations.