Theft of a Trade Secret Is Now a Federal Crime

By Ethan A. Brecher New York Law Journal May 7, 2007

Contrary to common wisdom, the legal jeopardy for an employee stealing his former employer's trade secrets goes well beyond the familiar civil lawsuit seeking an injunction and monetary damages.

Economic Espionage Act

The federal Economic Espionage Act of 1996 (EEA)1 is a "general criminal trade secrets" statute that criminalizes the theft or attempted theft of commercial trade secrets and conspiracies to steal such trade secrets.2 A conviction under the EEA can result in up to 10 years in a federal prison,3 $250,000 in fines for an individual and $5 million for an organization, criminal forfeiture as well as civil injunctive relief and restitution.4

The power of the EEA is that it criminalizes under federal law for the first time the theft of commercial trade secrets.5 The legislative history of the EEA indicates that it "was not designed to punish competition, even when such competition relies on the know-how of the former employees of a direct competitor. It was, however, designed to prevent those employees (and their future employers) from taking advantage of confidential information gained, discovered, copied, or taken while employed elsewhere."6

The EEA has generated some recent attention-grabbing headlines, such as the one on Feb. 1, 2007 from the U.S. Attorney for the Southern District of New York, who issued a press release stating: "Man Pleads Guilty to Stealing Morgan Stanley's Trade Secrets Relating to Hedge Funds."7 In this *Morgan Stanley* case, the defendant, a former Morgan Stanley employee, pleaded guilty to stealing Morgan Stanley's secret client lists identifying the hedge fund clients of its Prime Brokerage unit as well as formulas used to calculate rates paid by clients to Morgan Stanley for certain Prime Brokerage services. He sent those lists to another individual, also a former Morgan Stanley employee, for use in a consulting firm they were planning on starting.

The EEA was also used prominently in 2006 to prosecute Coca-Cola Co. employees who tried to sell Coke's trade secrets to PepsiCo.8

According to the US Department of Justice (USDOJ), since 2000 the government has prosecuted at least 37 EEA cases.9 Most of these prosecutions involved theft of trade secrets relating to computer software/computer code, engineering drawings/blueprints and medical products, but the prosecutions have also included such other diverse issues

as MasterCard's trade secrets being offered to Visa, trade secrets relating to Duracell's AA batteries10 and theft of proprietary pricing and customer information for a variety of businesses.

In a notable case from the securities industry involving retail stockbrokers, two brokers in Florida were each convicted of conspiracy to possess stolen trade secrets in violation of the EEA. One of the brokers gained access to a computer CD that had been stolen from First Union Securities Financial Network, Inc. (First Union Securities). The CD contained proprietary personal and financial information for a large number of First Union Securities' customers. The two brokers then used the stolen information to attempt to increase their brokerage client base. They also sold the stolen information to an undercover FBI agent. The broker who stole the CD was sentenced to 12 months and one day in prison, two years of probation, and was fined. The other broker was sentenced to two years of probation, fined, and ordered to forfeit ill-gotten gains. The U.S. Securities and Exchange Commission (SEC) also barred both brokers from the securities industry in a separate civil regulatory proceeding.11

Justice Department Manual

Just about any type of trade secret is subject to prosecution under the EEA, as is made clear by the USDOJ's Computer Crime & Intellectual Property Section, which issued a Manual in September 2006 for prosecutions under the EEA.12 Because the EEA's definition of a "trade secret" is derived from civil law and the Uniform Trade Secrets Act, civil law cases are "relevant to EEA prosecutions."13

The USDOJ's Manual, citing to a decision written by Judge Richard Posner of the U.S. Court of Appeals for the Seventh Circuit, explains that "[a] trade secret is really just a piece of information (such as a customer list, or a method of production, or a secret formula for a soft drink) that the holder tries to keep secret . . . , so that the only way the secret can be unmasked is by [unlawful activity]."14

The manual lists as trade secrets things as diverse as a computer software system used in the lumber industry; measurements, metallurgical specifications, and engineering drawings to produce an aircraft brake assembly; information involving zinc recovery furnaces and the tungsten reclamation process; information concerning pollution control chemicals and related materials; information regarding contact lens production; and pizza recipes.15

Under New York law, according to the New York Court of Appeals' decision in *Ashland Management Inc. v. Janien,* the definition of a "trade secret" is governed by §757 of the Restatement of Torts, which defines a "trade secret" as "any formula, pattern, device or compilation of information which is used in one's business and which gives him an opportunity to obtain an advantage

over competitors who do not know or use it."16 The Restatement suggests that in determining whether something is a "trade secret," several factors should be considered, including: "(1) the extent to which the information is known outside of [the] business; (2) the extent to which it is known by employees and others involved in [the] business; (3) the extent of measures taken by [the business] to guard the secrecy of the information; (4) the value of the information to [the business] and [its] competitors; (5) the amount of effort or money expended by [the business] in developing the information; and (6) the ease or difficulty with which the information could be properly acquired or duplicated by others."17 A trade secret must be secret, which is typically an issue of fact.18

In *Ashland,* the court held that an investment management firm's computerized mathematical stock selection model, based on six selected financial criteria which were evaluated according to various mathematical calculations, was not a trade secret but rather a promotional device. The court based this holding on the fact that, due to the firm's public disclosures, others could readily reproduce the mathematical calculations that were used to make the investment selections.

The New York Court of Appeals has also held that "customer lists" can be deemed to be trade secrets if the customers are not known generally in the industry, could only be discovered by extraordinary efforts and the list was developed through substantial expenditure of time and money.19

The EEA requires that a party take "reasonable measures to keep the information secret" in order for it to qualify for trade secret status.20

As such, the USDOJ Manual for EEA prosecutions provides that "prosecutors should determine what measures the victim used to protect the trade secret. These protections will be a critical component of the case or the decision not to prosecute. Typical security measures include: (1) keeping the secret physically secure in locked drawers, cabinets, or rooms, (2) restricting access to those with a need to know, (3) restricting visitors to secret areas, (4) requiring recipients to sign confidentiality, nondisclosure, or noncompetition agreements, (5) marking documents as confidential or secret, (6) encrypting documents, (7) protecting computer files and directories with passwords, and (8) splitting tasks among people or entities to avoid concentrating too much information in any one place."21

'United States v. Genovese'

In *United States v. Genovese,* the U.S. District Court for the Southern District of New York held that a trade secret could retain its secrecy despite a brief disclosure over the Internet: "[A] trade secret does not lose its protection under the EEA if it is temporarily, accidentally or illicitly released to the public, provided it does not become 'generally known' or 'readily ascertainable through proper means.'"22

In *Genovese,* the court rejected a challenge to the EEA on grounds that it was overbroad or vague. The defendant offered for sale on his own Web site the source code for two of Microsoft's operating systems (Windows NT 4.0 and Windows 2000), which had somehow appeared on the Internet. The defendant advertised the computer code for sale on his Web site, claiming that the source code was "jacked" and that it was hard to find elsewhere. An investigator hired by Microsoft bought the code from the defendant. Microsoft then contacted the FBI, which set up a sting operation and arrested the defendant after he sold the source code to an undercover agent.23 The court concluded that the defendant's own words indicated that he was on notice that the software source code had not been released publicly and derived value from its relative obscurity and recognized its scarcity even though it was available from other sources.24

Notably, "legal impossibility" is not a defense to a prosecution under the EEA. That is, a conviction is possible under the EEA for an attempted theft of a trade secret, even if the "trade secret" really isn't one. Thus, liability will attach so long as the government can prove beyond a reasonable doubt that an individual sought to acquire information he believed to be a trade secret, regardless of whether the information actually qualified as such, because a defendant's "culpability for a charge of attempt depends only on the circumstances as he believes them to be, not as they really are."25

The government can also prevail under the EEA even if the employee has not independently concluded that the information he took was in fact a "trade secret" as defined by the EEA. Instead, the government can secure a conviction if it can establish that an individual knew that the information was protected by proprietary markings, security measures, and confidentiality agreements, or knew or had a firm belief that the information was valuable to its owner because it was not generally known to the public, and that its owner had taken measures to protect it.26 On the other hand, a person cannot be prosecuted under the EEA if he took a trade secret because of ignorance, mistake, or accident, or he actually believed that the information was not proprietary after he took reasonable steps to warrant such belief.27

The EEA presents a number of practical but tremendously serious challenges for the practitioner. The potential for criminal prosecution under the EEA may result in difficult choices having to be made in a civil lawsuit involving trade secrets, including whether an individual should invoke his Fifth Amendment right against self-incrimination, even at the risk of subjecting himself to a default judgment for civil liability. On the other hand, the USDOJ states in its EEA Manual that "[n]otwithstanding the passage of the EEA, many disputes about trade secrets are still best resolved in a civil forum."28 Thus, although the deterrent effect of the EEA is great, the actual likelihood of being prosecuted under the EEA is not.

Moreover, because "legal impossibility" is not a defense under the EEA, an employee who might escape liability in the civil context for theft of a trade secret if it is ultimately determined that the subject matter in question was not a trade secret, might nonetheless be subject to criminal prosecution if he thought he was taking a trade secret. This fact could turn a hard won victory in a civil case establishing that the subject matter in question was not a trade secret into a wholly pyrrhic one if the employee is charged with attempted theft of a trade secret under the EEA.

Although there is no "advice of counsel" defense to the EEA,29 "advice of counsel" might negate an EEA defendant's mens rea.30 Because a defendant cannot be convicted under the EEA unless he knew or believed that he was misappropriating a trade secret in order to confer an economic benefit on himself or another person or entity, and that the offense would injure the owner of the trade secret, mens rea might be negated if counsel advised him either that the information in question was not a trade secret or that it was a trade secret to which he could claim ownership.31 Thus, counsel should take into consideration that the privilege covering any legal advice given to a client regarding the trade secret status of the subject matter in question might have to be waived in order for an individual to establish that he did not have the "guilty intent" that the government must prove existed in order to secure a conviction under the EEA.

Conclusion

The EEA has transformed an area of law that had been traditionally adjudicated through private civil litigation. Private employers now have the ability to turn to the federal government for help in pursuing former employees for the theft or attempted theft of their trade secrets. If they are successful in getting the attention of a federal prosecutor, employers are well-positioned to extract swift and potentially severe justice. As for employees considering taking their employer's trade secrets, they should reflect on the wisdom of doing so when the consequence might be a long prison sentence and hefty fines and other payments. It would also behoove employees to seek legal counsel before taking their employer's ostensible trade secrets in order to determine if what they want to take with them to a new employer is actually a trade secret.

When a client walks into a lawyer's office and seeks counsel in order to defend against a claim by his former employer that he stole trade secrets, he may have already committed a federal crime. A little advice can go a long way - and could also prevent hard time in a federal penitentiary and financial ruin.

Endnotes:

1. Pub. L. No. 104-294, 110 Stat. 3490 (1996) (codified at 18 USC §§1831- 1839). The "Theft of Trade Secrets" part of the EEA (18 USC 1832) provides

(a) Whoever, 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, knowingly (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information; (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information; (3) receives, buys, or possesses such information, knowing

the same to have been stolen or appropriated, obtained, or converted without authorization; (4) attempts to commit any offense described in paragraphs (1) through (3); or (5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both. (b) Any organization that commits any offense

described in subsection (a) shall be fined not more than $5,000,000. The EEA defines a "trade secret" to mean

all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if (A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through

proper means by, the public. 18 USC §1839(3).

2. The EEA also punishes those who knowingly misappropriate, or attempt to misappropriate, or attempt or conspire to misappropriate, trade secrets with the intent or knowledge that their offense will benefit a foreign government, foreign instrumentality, or foreign agent. 18 USC §1831. This part of the EEA,

which will not be addressed in this article, is designed to apply only when there is evidence of foreign government sponsored or coordinated intelligence activity. *U.S. v. Hsu,* 155 F. 3d 189, 195 (3d Cir. 1998).

3. 18 USC §1832(a).

4. 18 USC §§1832(a)(5) & (b), 1834, 1836(a). Restitution is available under the Mandatory Victims Restitution Act of 1996, 18 USC §3663A.

5. *U.S. v. Hsu,* 155 F. 3d at 194.

6. *U.S. v. Martin,* 228 F.3d 1, 11 (1st Cir. 2000), citing, H.R. Rep. No. 104- 788, at 7 (the EEA was meant to punish "the disgruntled former employee who walks out of his former company with a diskette full of engineering schematics.").

7. Press Release of the United States Attorney, Southern District of New York, Feb. 1, 2007; http://www.usdoj.gov/usao/nys/pressreleases/February07/chilowitzpleapr.pd f.

8. Press Release of the United States Attorney, Northern District of Georgia, Oct. 23, 2006; http://www.usdoj.gov/usao/gan/press/2006/10-23-06.pdf.

9. See http://www.usdoj.gov/criminal/cybercrime/ipcases.html#eea.

10. Press Release of the United States Attorney for Connecticut, Feb. 2, 2007, "Duracell Employee Pleads Guilty to Stealing Trade Secrets"; http://www.usdoj.gov/criminal/cybercrime/grandePlea.htm.

11. See *In Re Joseph Petrolino and Eric Siversen,* SEC Release No. 49578/April 19, 2004, http://www.sec.gov/litigation/admin/34-49578.htm.

12. See http://www.usdoj.gov/criminal/cybercrime/ipmanual/04ipma.html. 13. *Hsu,* 155 F. 3d at 196.

14. USDOJ Manual, citing, *ConFold Pac. v. Polaris Indus.,* 433 F.3d 952, 959 (7th Cir. 2006) (Posner, J.).

15. The USDOJ cited to the Court's decision in *Magistro v. J. Lou & Co.,* 703 N.W.2d 887, 890-891 (Neb. 2005), for the proposition that recipes for pizza dough and meat sauce could be deemed to constitute trade secrets. One assumes that the USDOJ listed the "pizza" trade secret for illustrative purposes only. Indeed, none of the cases listed on the USDOJ's website detailing the prosecutions under the EEA indicate that the EEA has been used against anyone who stole or tried to steal a pizza recipe.

16. See *Ashland Management Inc. v. Janien,* 82 N.Y.2d 295, 624 N.E.2d 1007, 604 N.Y.S.2d 912, 917-918 (1993).

17. Id. 18. Id.

19. *Leo Silfen Inc. v. Cream,* 29 N.Y.2d 387, 392, 328 N.Y.S.2d 423, 278 N.E.2d 636 (1972); *Shmueli v. Corcoran Group,* 9 Misc.3d 589, 802 N.Y.S.2d 871 (N.Y. Sup., 2005) (issue of fact as to whether customer list containing names, addresses, and telephone numbers of prior and prospective real estate purchasers was a trade secret).

20. 18 USC 1839 (3)(A); *United States v. Lange,* 312

F.3d 263, 266 (7th Cir. 2002).

21. USDOJ Manual, Section IV.B.3.a.vii, p.148-149 ("A defendant who was unaware of the victims' security measures can be convicted under the EEA if he was aware that the misappropriated information was proprietary). *United States v. Krumrei,* 258 F.3d 535, 538-39 (6th Cir. 2001) (rejecting void-for- vagueness argument against EEA); accord *United States v. Genovese,* 409 F.Supp.2d 258 (S.D.N.Y 2005) (rejecting void-for-vagueness challenge to EEA indictment). But see id. (noting that the defendant could argue that he was unaware of the victim's security measures at trial).").

22. 409 F.Supp.2d 253, 257 (SDNY 2005) (citing 18 USC §1839 (3)(B)).

23. In a sly acknowledgement of the defendant's use of slang, the Court noted that it interpreted the word "jacked" as an abbreviation for "hijacked" and cited approvingly to an article on the Internet that discussed how the video game "Grand Theft Auto" (which glorifies auto-theft and other mayhem) had itself been "jacked" a week before it was released for sale and republished on the Internet. *Genovese,* 409 F.Supp.2d at 257 n. 3.

24. 409 F.Supp.2d at 257.

25. *Hsu,* 155 F.3d at 203; *U.S. v. Yang,* 281 F.3d 534 (6th Cir. 2002). "Legal impossibility" is also not a defense to a charge of conspiracy. *Hsu,* 155 F.3d at 203.

26. See USDOJ Manual at IV.B.5.b. p. 155. The government also need not prove that the employee acted out of malice or evil intent. Rather, the government need show "merely that the actor knew or

was aware to a practical certainty that his conduct would cause some disadvantage to the rightful owner." H.R. Rep. No. 104-788, at 11-12 (1996), reprinted in 1996 USCC.A.N. 4021, 4030. See also USDOJ Manual at IV.B.5.b. p. 157.

27. USDOJ Manual at IV.B.3.c, p. 155, citing, 142 Cong. Rec. 27, 117 (1996) ("This [knowledge] requirement should not prove to be a great barrier to legitimate and warranted prosecutions. Most companies go to considerable pains to protect their trade secrets. Documents are marked proprietary; security measures put in place; and employees often sign confidentiality agreements.").

28. USDOJ Manual at IV.C.5 p. 163.

29. USDOJ Manual at IV.C.4, p. 162-163; *U.S. v. Urfer,* 287 F.3d 663, 666 (7th Cir. 2002) (Posner, J.).

30. "Mens rea" is defined as: "A guilty mind; a guilty or wrongful purpose; a criminal intent. Guilty knowledge and willfulness." Black's Law Dictionary at 510 (West Publishing Co. 1983).

31. USDOJ Manual at IV.C.4, p. 162-163 ("To rely on advice of counsel at trial, the defendant must first provide "independent evidence showing (1) the defendant made full disclosure of all material facts to his or her attorney before receiving the advice at issue; and (2) he or she relied in good faith on the counsel's advice that his or her course of conduct was legal." *Covey v. United States,* 377 F.3d 903, 908 (8th Cir. 2004) (citations and alterations omitted); see also *United States v. Butler,* 211 F.3d 826, 833 (4th Cir. 2000) (same)." See also *Hsu,* 155 F.3d at 196 ("[The EEA 18 USC] §1832 states that the defendant must intend or

know that the offense will injure an owner of the trade secret . . . . The legislative history indicates that this requires 'that the actor knew or was aware to a practical certainty that his conduct

would cause such a result.' S. Rep. No. 104-359, at 15.").