TRADE SECRETS AND THE FEDERAL CRIMINAL LANDSCAPE: THE ECONOMIC ESPIONAGE ACT OF 1996

January 22, 2009

Kevin Di Gregory, Partner
Becky Walker, Partner

History and Background

- "What do you do with a General when he's through being a General?" – Irving Berlin
- "The end of the Cold War sent government spies scurrying to the private sector to perform illicit work for businesses and corporations." –*United States v. Hsu*, 155 F.3d 189,194 (3d Cir. 1998) (citing legislative history of EEA).
- Global marketplace
- No comprehensive federal statute dealing with trade secret theft until...

Economic Espionage Act 18 U.S.C. 1831, et.seq.

- Signed into law in 1996
- Criminalizes two types of trade secret misappropriation:
  - Economic Espionage (foreign government sponsored)
  - Commercial Trade Secret Theft
- "The Usual Suspects"
  - Employee steals for his own benefit, to harm the owner or both
  - Domestic or foreign competitor, or foreign government, steals to gain an economic advantage

18 U.S.C. 1831 (Economic Espionage)

- Intent to benefit foreign government
- Unauthorized misappropriation or knowing receipt
- Knowledge that information was proprietary
- Trade secret
- Attempt to steal trade secret
- Conspiracy to steal trade secret
- 15 years/$500,000 fine
- Organizations can be fined up to $10 million

18 U.S.C. 1832 (Trade Secret Theft)

- Intent to convert
- Information that was proprietary
- Trade secret
- Related to product placed in or planned for interstate or foreign commerce
- For the economic benefit of another
- Intending economic harm or knowing economic harm will come to owner
- 10 years/$250,000 fine
- Organizations can be fined up to $5 million

Massive Scope of the Problem and Prevalence of the Enemy Within

- According to a 2006 report issued by the United States Trade Representative, U.S. companies are losing $250 billion annually due to trade secret theft
- According to the 2007 E-Crime Watch Survey conducted by Carnegie-Mellon University, the U.S. Secret Service and Microsoft, nearly 50% of data security attacks were inside jobs

Trade Secret

- Defined at 18 U.S.C. 1839(3)
  - "all forms and types of financial, business, scientific, technical, economic, or engineering information"
  - "whether tangible or intangible"
  - "whether or how stored, compiled or memorialized"
  - "if the owner ... has taken reasonable measures to keep ... secret"
  - "if ... information derives economic value ... from not being generally known to, and not being readily ascertainable through proper means by, the public"

Forfeiture and Restitution

- 18 U.S.C. § 1834
  - Mandatory: proceeds
  - Discretionary: instrumentalities
- 18 U.S.C. § 3663A
  - Mandatory Victims Restitution Act (MVRA)
  - Includes trade secret theft victims

Extraterritoriality

- Defined at 18 U.S.C. 1837
- Applies to conduct outside U.S. if offender is:
  - Citizen or permanent resident alien of U.S., or
  - Organization organized under U.S. law

Targeted Trade Secrets

- Formulas
- Computer Source Code
- Customer Business Development Information
- Design Specs
- Business Software
- Biomedical Research

Victim Companies

- Avery Dennison
- Bristol-Myers
- Pittsburgh Plate Glass
- Cleveland Clinic Foundation
- Kodak
- Lucent Technologies
- Sun Microsystems
- Lockheed Martin
- DirecTV
- Harvard Medical School
- Intel Corporation
- MasterCard
- Cisco Systems
- Gillette
- ICS, Deloitte & Touche

....even Coca-Cola®

- "A federal jury rejected a former Coca-Cola secretary's claim that she was duped by two accomplices and convicted her ... of conspiring to steal trade secrets from the world's largest beverage maker in an effort to sell them to its rival, Pepsi."
  - New York Times, February 3, 2007

Defenses

- Parallel development
- Reverse engineering
- Not a trade secret
  - generally available to, or readily ascertainable by the public
  - information not properly protected
- Advice of counsel to negate intent

Impossibility NOT a Defense

- Impossibility is not a defense to attempted trade secret theft or conspiracy to commit trade secret theft
  - "If we were to conclude that legal impossibility were a defense to the attempted theft of trade secrets, the government would have to use actual trade secrets in undercover operations...Congress could not have intended such a result, in as much as it was striving to prevent economic espionage and to maintain the confidentiality of trade secrets." *United States v. Hsu*, 155 F.3d 189, 202 (3d Cir. 1998)

Confidentiality

- 18 U.S.C. 1835
  - "the court ***shall*** enter such orders and take such other actions as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws."
  - Government has right to interlocutory appeal if disclosure of trade secret ordered
- Fed. R. Crim. P. 16 (d)(1) Protective Orders

Discovery

- Fed. R. Crim. P. 16(a)(1)(E)
  - Upon the request of the defendant the government is obligated to provide any documents it intends to use in its case-in-chief *or if the item is material to the preparation of the defense.*

Evidence

- Fed. R. Evid. 402
  - "All relevant evidence is admissible"
- Fed. R. Evid. 401
  - "Relevant evidence means evidence having ***any*** tendency to make the existence of ***any*** fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence."

Sixth Amendment

- Confrontation clause
  - Defense
    - Without disclosure of trade secret, defendant will be unable to effectively cross-examine government witnesses
- Compulsory process clause
  - Offense ("Graymail")
    - Trade secret must be disclosed because its affirmative use is essential to the defense
- Right to a public trial

Unresolved Issue on Confidentiality: Footnote 15

- "We emphasize that we need not reach and are not determining…whether the disclosure of trade secrets is mandated by the Constitution or the Federal Rules of Criminal Procedure if a defendant is charged with the actual theft of trade secrets. This is a complex issue." *United States v. Hsu,* at n.15

Federal Prosecution As An Alternative or Supplemental Remedy For the Victim: PROS

- Deterrence
  - Insiders
  - Competitors
- Most effective against disgruntled former or current employees without deep pockets

Deterrence: Go Directly to Jail, Do Not Pass Go, Do not Collect $200

- "Former DuPont Scientist Sentenced for Trade Secret Theft"
  - "As a science company, DuPont takes aggressive measures to protect its unique and confidential technologies....Judge Robinson underscored the importance of those actions by sentencing Mr. Min to federal prison and sent a clear signal to others who might consider committing similar crimes."
    - Information Week, November 8, 2007, quoting DuPont's General Counsel

Federal Prosecution CON: Loss of Control

- U.S. Attorney and FBI control the investigation and the evidence, including the trade secret
- Trade secret may be ordered disclosed during discovery or at trial

When Victimized Minimize the Risks of Reporting

- Report as soon as possible
  - Early reporting of the theft of trade secrets may allow the FBI to establish an undercover operation using documents that appear to be trade secrets but are not actual trade secrets.
  - "The Yangs believed that the information Lee was providing was trade secrets belonging to Avery. The fact that they actually did not get a trade secret was irrelevant." *United States v. Yang*, 281 F.3d 534, 543-544 (6th Cir. 2002).

Minimize the Risk of Reporting

- Seek a meeting with the prosecutor
  - Prosecutor may not be familiar with EEA
  - Emphasize economic value and efforts to maintain secrecy
  - Discuss confidentiality and protective orders
    - DOJ Manual "strongly encourage[s]" AUSAs to take whatever steps are necessary to protect trade secrets
  - Discuss redactions to or substitutions for the documents containing trade secrets
  - Discuss injunctive relief provided for at 18 U.S.C. 1836
  - Discuss other potential charges, such as conspiracy, attempt, mail fraud, wire fraud, unlawful access to a protected computer to commit fraud or to obtain information, interstate and foreign transportation of stolen property

Reasonable Measures to Maintain Secrecy

- What DOJ will consider when evaluating:
  - Physical security
  - Employee training
  - "Need to know" access
  - Computer security like passwords and encryption
  - Document markings – **"CONFIDENTIAL"**
  - Confidentiality, nondisclosure or non-competition agreements
  - Splitting tasks
- Reasonableness dependent on facts of each case.

Redactions and Substitutions

- In cases where completed theft is charged, Court may allow the trade secret information to be redacted from documents to be introduced into evidence or allow non-confidential substitutions or summaries to be presented to the jury.
  - See *United States v. Hsu*, 982 F.Supp. 1022 (E.D. Pa 1997); *United States v,.Hsu*, 155 F.3d 189 (3rd Cir. 1998);*United States v. Hsu*, 185 F.R.D. 192 (E.D. Pa. 1999)

Injunctions

- 18 U.S.C. 1836 provides that the United States may seek an injunction:
  - prevent further disclosure of trade secret during pending criminal investigation
  - in lieu of criminal prosecution
  - U. S. district courts have exclusive jurisdiction
- Internal DOJ guidance calls for injunctive relief to be sought where "defendant's conduct does not warrant...prosecution."

Alternative or Additional Charges

- Computer Fraud and Abuse Act, 18 U.S.C. §1030 (a)(2):
  - Intentional, unauthorized access to obtain information or exceeding authorized access
  - Information does not have to be trade secret or even confidential
- Wire Fraud, Mail Fraud, 18 U.S.C. §§1341, 1343, 1346 (honest services fraud)
  - 1341, 1343: obtaining intangible property can be object of scheme to defraud
  - 1346: breach of fiduciary duty by misappropriation
- Interstate and Foreign Transportation of Stolen Property, 18 U.S.C. § 2314
  - "Property" includes electronic files containing images, plans, formulas, etc., but trade secret status irrelevant to proof of crime

Confidentiality: The Rest of Footnote 15

- "[W]hether the information qualifies as an actual 'trade secret' is precisely defined by the EEA, and centers on such factual questions as how the information has been guarded by its owner and whether it is ascertainable by the public, rather than on the content of the secret...This raises an issue as to whether the information or formula itself is in fact material to the existence of the trade secret." *United States v. Hsu*, 155 F.3d 189, at n.15 (3rd Cir. 1998)

Analogy to National Security Cases

- 18 U.S.C. App. 3, The Classified Information Procedures Act (CIPA)
- Allows the court to authorize the government to redact classified information or substitute unclassified summaries in discovery documents
  - CIPA, section 4
- Allows the court to order substitutions and summaries in lieu of the disclosure of classified information, "if it finds that the statement or summary will provide the defendant with substantially the same ability to make his defense..."
  - CIPA, section 6(c)

Not a Violation of the EEA

- Employees general knowledge and skill
- Employees exposure to trade secrets
  - Changes employers
  - Starts own business
- Competition not reliant on trade secrets

Not a Violation of the EEA

- "The government cannot prosecute an individual for taking advantage of the general knowledge and skills or experience that he or she obtains or comes by during his tenure with a company. Allowing such prosecutions to go forward and allowing the risk of such charges to be brought would unduly endanger legitimate and desirable economic behavior."
  - 142 Cong. Rec. S12201, 12213 (daily ed., Oct. 2,1996)

Attorney General Oversight

- AG or designee required by Congress to approve the initiation of prosecutions for the first 5 years of the EEA
- DOJ has maintained the approval requirement for 18 U.S.C. 1831 prosecutions

DOJ Activity 2008

- *United States v. Cartwright, et al.*, D. Md.
  - Indicted January 7, 2008
  - Guilty Pleas July 29, 2008
- *United States v. Zeng*, SDTX
  - Indicted February 21, 2008
  - Convicted and Sentenced May 15, 2008
- *United States v. Cotton*, EDCA
  - Guilty plea February 29, 2008
  - Sentenced May 16, 2008
- *United States v. Kim*, NDOH
  - Indicted March 26, 2008
- *United States v. Jin*, NDIL
  - Indicted April 2, 2008
- *United States v. Nosal and Christian*, NDCA
  - Indicted April 10, 2008
- *United States v. Malhorta*, NDCA
  - Guilty Plea July 11, 2008
- *United States v. Lockwood, Haehnel, and Liu*, E.D. Mi.
  - Guilty pleas September 15, 2008
- *United States v. Pani*, D. Mass.
  - Indicted November 5, 2008
- *United States v. Shin, et al.*, NDOH
  - Indicted November 12, 2008

DOJ Activity 2009 and Beyond

- **"Prevent Corporate Cyber-Espionage:** Work with industry to develop the systems necessary to protect our nation's trade secrets and our research and development. Innovations in software, engineering , pharmaceuticals and other fields are being stolen online from U.S. businesses at an alarming rate."
  - The Obama-Biden Transition Team http://change.gov/agenda/homeland_security_agenda/

Further Information

- Becky Walker
  - BSWalker@manatt.com
  - 310.312.4130
- Kevin Di Gregory
  - Kdigregory@manatt.com
  - 202.585.6564

Further Reading

- *War By Other Means: Economic Espionage in America,* by John Fialka. New York: W. W. Norton & Co., Inc., 1997
- *Economic Espionage and Industrial Spying,* by Hedieh Nasheri. New York: Cambridge University Press, 2005 (reprinted 2008)