Insider Threats to Your Trade Secrets: Prevention and Response

Trisha Anderson, Robert Haney, Dan Johnson

April 9, 2019

COVINGTON

BEIJING BRUSSELS DUBAI FRANKFURT JOHANNESBURG LONDON LOS ANGELES
NEW YORK PALO ALTO SAN FRANCISCO SEOUL SHANGHAI WASHINGTON

www.cov.com

Introduction

Presenters

Trisha B. Anderson
tanderson@cov.com

Robert P. Haney Jr.
rhaney@cov.com

Daniel E. Johnson
dejohnson@cov.com

Agenda

- Avoiding theft of trade secrets by employees, contractors and others
- Litigation and other actions to consider when the secret may be out
- Partnering with the government to respond to insider threats and theft
- Recent developments in trade secret law and insider threats
- Q&A

Avoiding Trade Secret Theft

What is a Trade Secret?

- Your data may be a trade secret ("TS") if:
  - It is commercially valuable to you; ***and***
  - You take "reasonable" steps to keep it secret

- Examples of potential TS:
  - Formulas
  - Compilations
  - Customer intelligence
  - Designs
  - Processes/techniques
  - Business plans
  - Financial data

Novelty and Absolute Secrecy Are Not Required

- Unlike patentable technology, a TS need not be "novel"
  - Two competitors can have essentially the "same" TS
  - However, information that is "readily ascertainable" by outsiders is not protectable as a TS
- Secrecy is key, but absolute secrecy is not required
  - TS owner must take "reasonable" steps under the circumstances to preserve the secrecy of the data
  - Limited disclosure is permissible under certain circumstances
  - Failure to take reasonable steps destroys TS protection

Threats to Your TS

- TS theft is estimated to cost U.S. businesses
  - >$300 billion per year
  - >2.1 million jobs per year
- U.S. Congress recognized the importance of TS protection in the Defend Trade Secrets Act of 2016 (“DTSA”)
- Most TS threats/thefts are by insiders
  - Current and former employees
  - Customers, suppliers, manufacturers

TS Protection Program

- Develop a written policy for protection of confidential data, including TS
- Identify the data to be protected
  - Patent v. TS
  - Explain to those given access how to protect the TS
  - Consider marking/stamping the TS
- Train employees and consultants
  - What should be protected
  - How to protect it
  - The importance of secrecy
- Document TS developments
  - E.g., lab notebooks
  - Require reporting of developments

TS Protection Program

- Limit access on a “need-to-know” basis
- Require those who have access to the data to sign an appropriate NDA
  - Employees, consultants, customers, potential customers, teammates, manufacturers, suppliers
  - Be mindful of enforceability
    - Avoid overbroad and illegal restrictions
    - Reference DTSA immunity
  - Include a workable mode of identifying data covered by the NDA
- Understand third-party data rights and obligations

TS Protection Program

- Maintain physical and information systems security
- Monitor and audit compliance with your TS protection program. For example:
  - Has everyone with access to the TS signed your NDA?
  - Are all TS appropriately designated/marked?
- Immediately correct inadvertent disclosures

Avoiding Insider Threats

- Beware the rogue applicant, supplier or customer
- Manage your staff
- Monitor employee activity
  - Follow privacy laws
  - Have any employees engaged in unusual access/copying?
- Follow strict exit procedures
  - Retrieve your devices and data (including from personal devices)
  - Monitor past activity for suspicious behavior
  - Reiterate confidentiality obligations
  - Obtain certification that all data was returned
  - Consider sending a “shot across the bow”

Civil Litigation Options

Incident Response Plan

- Consult “Incident Response Plan”—*which has been created ahead of time*
- Internal communication / escalation plan
  - Working group of point people from IT, Legal, HR, IR, senior management, Board, PR, etc.
- Preserve the evidence
  - Revoke access to information
  - Hire forensics expert?
- Consider hiring outside counsel
- Determine scope of internal investigation

Strategic Considerations in Civil Litigation

- Potential to obtain injunctive relief, in addition to damages
- Send a strong message that company will protect its IP
- Lower burden of proof than in criminal cases
- Discovery may reveal co-conspirators to sue
- Need to decide if the importance of the information taken justifies the investment of time and money in litigation
- Risk of moving too quickly and mis-defining the trade secret
- Need to use the time of highly specialized employees

Strategic Considerations in Civil Litigation

- Choice of law and choice of forum
  - Absent a contractual choice of law clause, law of the state of employment generally applies
  - Uniform Trade Secrets Act ("UTSA") applies in most states (New York is an exception)
  - Federal court or state court
  - DTSA and option for Federal jurisdiction
- Defining the trade secret in litigation
  - Too broad: information may not qualify as a trade secret
  - Too narrow: reduces the value of claims
- UTSA states: tort claim or misappropriation claim?

Lex Machina's Trade Secret Litigation Report 2018 (2009 to 2018 Q2)

- In 2017, federal district court filings increased 30% over filing is 2016, the year DTSA passed
- When courts rule on the merits of a motion for injunction, the grant/deny rates tend to favor plaintiffs
- Existence of a protectable trade secret is difficult to prove at summary judgment, which is some basis for the trend favoring defendants at summary judgment (64% defense win)
- Trials tend to favor plaintiffs (72% plaintiff win rate)

Defend Trade Secrets Act of 2016

- Bipartisan legislation passed and signed into law in 2016
- Adopts UTSA and establishes federal trade secret misappropriation civil claim
- Federal court may in "extraordinary circumstances" order *ex parte* seizures
  - Law enforcement to enter land and seize property "necessary to prevent the propagation or dissemination of the trade secret"
  - Applicant must post a bond sufficient to cover damages if the seizure turns out to be wrongful; target can get damages if the seizure turns out to be wrongful

Ex Parte Seizure Under the DTSA

- Courts are reluctant to grant *ex parte* seizure
  - Courts have denied requests for *ex parte* seizure in the vast majority of cases decided thus far
  - Courts often find that ordinary injunctive relief is adequate

- *Ex parte* seizure has been granted in three cases so far
  - Courts are requiring a showing of a risk of destruction of evidence
  - E.g., *Mission Capital Advisors, LLC v. Romaka*, No. 16-cv-05878 (S.D.N.Y. July 29, 2016)
  - After initially denying an ex parte seizure, the defendant avoided service of a TRO order and failed to appear for a hearing
  - The court ordered that U.S. Marshals seize the trade secrets from his personal computer

Recent DTSA Seizure Cases

- *Solar Connect, LLC v. Endicott*, No. 2:17-CV-1235, 2018 WL 2386066 (D. Utah Apr. 6, 2018)
  - The court granted a civil seizure order where defendants: had "a high level of computer and technical proficiency"; had attempted to delete data from their computers; had "shown a willingness to provide false and misleading information"; and had "shown a willingness to hide information and move computer files rather than comply with requests to cease use of Plaintiff's proprietary materials."
  - The order required seizure of the defendants' computers and other devices and the copying of files from cloud storage accounts. The court also required that defendants provide any usernames and passwords associated with the devices and accounts.

Recent DTSA Seizure Cases (Continued)

- Order [doc. 17], *Vice Capital, LLC v. CBD World, LLC*, No. 5:18-cv-00566-D (W.D. Okla. June 20, 2018)
  - The court granted a seizure order, finding that it was likely defendants "would evade, avoid, or otherwise not comply with such an order." Defendants had backed out of a franchisee relationship and continued to use plaintiff's trade secrets, despite a cease and desist letter. Defendants had also exported a customer list and threatened to send a message to customers claiming that plaintiffs' products were tainted and would make their customers sick. The court further found that there was a high likelihood that defendants would "delete, secure, move, copy, or obscure" the trade secrets without a seizure order.
  - The court ordered the U.S. Marshal to seize any devices that belonged to the defendants that were used in relation to defendants' business. The court also authorized seizure of defendants' cloud storage usernames and passwords. To minimize the seizure's effect on defendants' business, the plaintiffs agreed to provide defendant with replacement devices during this period.

Recent DTSA Seizure Cases (Continued)

- Order [doc. 6], *Thoroughbred Ventures, LLC v. Disman*, No. 4:18-CV-00318, 2018 WL 3752852 (E.D. Tex. Aug. 8, 2018)
  - The court granted a seizure order where it was likely defendant would "destroy, move, or hide" the computer containing the trade secrets. Defendant had downloaded various trade secrets onto his personal device in violation of an employment agreement, and had failed to return the information to plaintiffs upon request. There was also evidence defendant was using this information to engage in investment opportunities. The court found that seizure was necessary because without it, defendant "would be free to continue to solicit Plaintiff's investors to propagate his real estate investment scheme in breach of his Employment and Confidentiality Agreement."
  - The court ordered the Marshals to seize the specific HP Laptop containing the trade secrets

Partnering with the Government

Enforcement of Trade Secret Theft

- Most criminal enforcement is federal
  - Economic Espionage Act ("EEA"), 18 U.S.C. § 1831-1839
  - Depending on the facts, other criminal statutes could apply:
    - Espionage Act, 18 U.S.C. § 793
    - National Stolen Property Act, 18 U.S.C. § 2314
    - Computer Fraud and Abuse Act, 18 U.S.C. § 1030
    - Wire Fraud, 18 U.S.C. § 1343
    - Attempt and Conspiracy, 18 U.S.C. § 1349
    - Money Laundering, 18 U.S.C. § 1956

- Some state-level criminal enforcement
  - New York: Unlawful Use of Secret Scientific Material, New York Penal Law § 165.07
  - California: Theft of Electronic Data, California Penal Code § 502

Economic Espionage Act

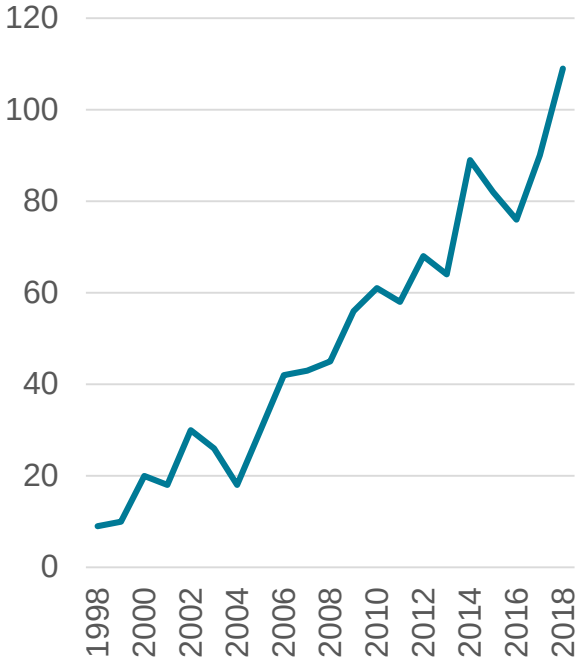
- Economic Espionage Act
  - Overview: Criminalizes stealing, unauthorized copying, and receipt of trade secrets known to be unlawfully acquired
  - Key Provisions:
    - 18 U.S.C. § 1831: Criminalizes foreign economic espionage; requires that the theft of the trade secret be done to benefit a foreign government, instrumentality, or agent
    - 18 U.S.C. § 1832: Criminalizes commercial theft of trade secrets, regardless of who benefits
  - Penalties:
    - Individuals: Fine of up to $5M + up to fifteen years imprisonment
    - Corporations: Fine up to $10M or three times the value of the stolen information

Elements: Economic Espionage

Economic Espionage 18 U.S.C. § 1831(a)(3)	Commercial Theft of Trade Secrets 18 U.S.C. § 1832(a)(3)
1. The defendant intended or knew his actions would benefit a foreign government, instrumentality, or agent.	1. The defendant intended to covert a trade secret to the economic benefit of anyone other than the owner.
2. The defendant knowingly received, bought, or possessed a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization.	2. The defendant knowingly received, bought, or possessed a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization.
3. The information was a trade secret.	3. The information was a trade secret.
N/A.	4. The defendant intended, or knew, the offense would injure the owner of the trade secret.
N/A.	5. The trade secret was related to or included in a product that is produced for or placed in interstate or foreign commerce.

Recent Trends in Economic Espionage

Indictments on the rise

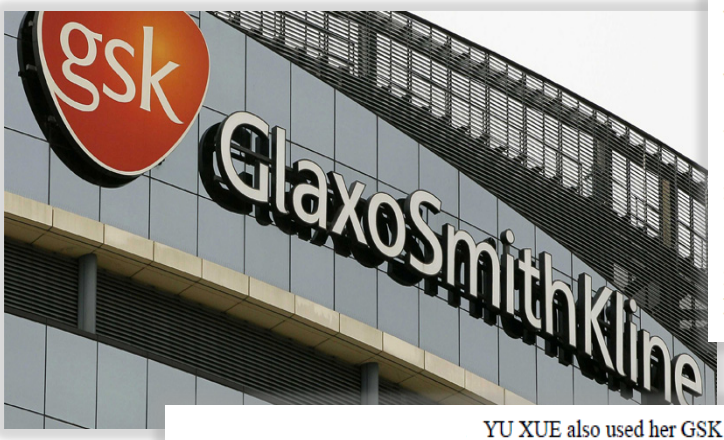


Key facts and figures

- Costs the U.S. economy billions of dollars annually
- In the past, targeted mostly at defense-related and high-tech industries
- In recent years, cases have shown that no industry is immune

Criminal Enforcement: Recent Case

- *United States v. Xue* (E.D. Pa. 2018)



VIOLATIONS:
18 U.S.C. § 1349 (conspiracy to commit wire fraud – 1 count)
18 U.S.C. § 1832(a)(5) (conspiracy to steal trade secrets - 1 count)
18 U.S.C. § 1956(h) (conspiracy to commit money laundering – 1 count)
18 U.S.C. § 1343 (wire fraud – 16 counts)
18 U.S.C. § 1832(a) (theft of trade secrets – 24 counts)
Notices of Forfeiture

YU XUE also used her GSK computer to download a substantial amount of trade secret information from GSK's network onto a thumb drive or other portable storage device in order to send this information to TAO LI, YAN MEI, and others. YU XUE, TAO LI, and YAN MEI founded Renopharma, Inc., Nanjing Renopharma, Ltd., and Shanghai Renopharma, Ltd., (hereinafter collectively known as "RENOPHARMA") to market and sell the stolen trade secret and otherwise confidential information.

Criminal Enforcement: Other Recent Cases

- *United States v. Wei Pang, et. al* (N.D. Cal. 2015)

- *United States v. Walter Liew, et. al* (N.D. Cal. 2011)

- *United States v. Wang Dong, et. al* (W.D. Pa. 2014)

- *United States v. Pu* (N.D. Ill. 2014)

Outreach to Law Enforcement: Possible Benefits

- Powerful investigative tools (e.g., warrants) may be available
- Criminal authorities may be able to take action quickly in urgent circumstances
- Government bears the costs of the investigation and prosecution
- If government prosecution succeeds, collateral estoppel can have civil benefits
- Signals that the company is acting responsibly and will aggressively protect its IP

Outreach to Law Enforcement: Possible Downsides

- The company may have limited control over how the matter is ultimately investigated and prosecuted
- Meaningful information sharing may generally flow only from the company to law enforcement
- Can occupy company resources and time for years, including requiring depositions and/or testimony of current or former employees
- Risk that sensitive company information will become exposed in the course of its investigation

Who Are The Law Enforcement Contacts?

- Most trade secret investigations are handled by the FBI
  - Who handles the case? Once trade secret theft is reported:
    - The investigation is generally—but not always—handled by the local field office of the company's home jurisdiction
    - Specialized subject matter experts may also be involved, regardless of their field office (e.g., experts in specific counterintelligence targets)
  - Who at the FBI receives reports? Ultimately, the FBI can route investigations internally, and often does. Some options for making reports:
    - Local field office or regional groups in the company's home jurisdiction
    - The FBI Tip Line
    - The company's existing FBI contacts

Who Are The Law Enforcement Contacts?

- Other agencies may also be involved in certain circumstances
  - Intelligence Community agencies, when the trade secret theft implicates national security concerns
  - Defense Department agencies, particularly when the trade secret theft impacts U.S. government contractors, their subcontractors, or suppliers
  - Other civilian agencies (e.g., DHS, Treasury) when their specific missions are related to the trade secret theft

- If you don't know who to call, outside counsel can help
  - Established relationships with many agencies
  - Extensive experience and contacts in both the criminal and national security / counterintelligence contexts

Questions?

Presenters

Trisha B. Anderson
tanderson@cov.com

Robert P. Haney Jr.
rhaney@cov.com

Daniel E. Johnson
dejohnson@cov.com