MORRISON FOERSTER

CIPLA
CLEVELAND • AKRON • CANTON

TRADE SECRETS AT THE ITC: THE AFTERMATH OF TIAN RUI

Mark L. Whitaker

Tuesday, March 23, 2021

Who Cares About Trade Secrets?

THE WALL STREET JOURNAL.

POLITICS

Senate Passes Trade-Secrets Bill

Legislation authorizes companies to take trade-secret disputes directly to federal court

By Siobhan Hughes
April 4, 2016 6:12 pm ET

The bill passed 87-0 in a rare moment of political agreement.

The New York Times

Star Technologist Who Crossed Google Sentenced to 18 Months in Prison

Anthony Levandowski, a onetime star Silicon Valley engineer of self-driving cars, had pleaded guilty to stealing trade secrets.

By Kate Conger

Aug. 4, 2020

Common Scenarios

- Key technical employee moves to competitor
- Employees leave *en masse* to join competitor
- Joint development project ends; partner then announces product based on your information
- Former partner applies for patents based on joint R&D work
- Vendor starts selling product based on your information
- Competitor sends demand letter after you hire new employee

Recent Policy and Legislation

UNITED STATES: DEFEND TRADE SECRETS ACT (MAY 2016)

- The **Defend Trade Secrets Act of 2016** (**DTSA**) (Pub.L. 114–153, 130 Stat. 376, enacted May 11, 2016, codified at 18 U.S.C. § 1836, et seq.) is a United States federal law that allows an owner of a trade secret to sue in federal court when its trade secrets have been misappropriated. The act was signed into law by President Barack Obama on May 11, 2016. It underscored Congress's desire to align closely with the Uniform Trade Secrets Act, which had been adopted in some form in almost every U.S. state. Technically, the DTSA extended the Economic Espionage Act of 1996, which criminalizes certain trade secret misappropriations.
- The law also grants legal immunity to corporate whistleblowers.

EUROPEAN UNION:

- The EU Trade Secrets Directive, officially titled "Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure" (the "**TSD**"), is a legal instrument by the European Union (EU) that is intended to harmonize the currently fragmented laws regarding trade secrets across the EU Member States. While the TSD does not have direct legal effect, each of the Member States are required to transpose the TSD into its respective national laws by June 9, 2018.

The Basics

ANYTHING CAN BE A TRADE SECRET

- Formulas
- Processes
- Methods of doing business
- Abstract ideas

IT HAS TO BE SECRET

- Limit access and dissemination
- Use and enforce NDAs
- Follow appropriate employment practices
  - Offensive
  - Defensive

- **Trade secret protection does not protect you from others figuring out the information on their own**
- **Trade secret protections are about the process as much as the idea**

What is a Trade Secret?

"TRADE SECRET"

(D) "Trade secret" means information, including the whole or any portion or phase of any scientific or technical information, design, process, procedure, formula, pattern, compilation, program, device, method, technique, or improvement, or any business information or plans, financial information, or listing of names, addresses, or telephone numbers, that satisfies both of the following:

(1) It **derives independent economic value**, actual or potential, from **not being generally known to, and not being readily ascertainable by proper means** by, other persons who can obtain economic value from its disclosure or use.

(2) It is the subject of **efforts that are reasonable under the circumstances to maintain its secrecy.**

Ohio Uniform Trade Secrets Act (Ohio Revised Code §§1333.61-69 (1994))

"Economic Advantage"

- Includes actual or potential economic value
  - Potential economic value means that even if no market currently exists for a product, a significant market could exist in the future
- Thus, a trade secret would include the currently valuable recipe for Coca-Cola, as well as a yet-to-be marketed revamped recipe for Coke II
- Includes information that affords only "slight" economic value to the holder
- Includes information that has economic value from a negative viewpoint.
  - For example, the results of research studies showing that a process will not work

Not "Generally Known" or "Readily Ascertainable"

- Whether competitors of the trade secret holder actually know or can easily discover the secret
- Trade secrets may include combinations of elements that are in the public domain, if the trade secret constitutes a unique, effective, successful and valuable integration of public domain information
  - For example, a customer list may include names and phone numbers that are publicly available; however, a competitor would save time and money by accessing this previously compiled list
- Just because something exists on the Internet does not mean that it is "fair game," especially if it was not lawfully published on the Internet

"Reasonable Efforts to Maintain Secrecy"

- The extent of the security measures taken by the owner of the trade secret need not be absolute, but must be reasonable under the circumstances, depending on the facts of the specific case. Heroic measures are not necessary.

- The owner of the material must assess the value of the material it seeks to protect, the extent of a threat of theft, and the ease of theft in determining how extensive their protective measures should be.

- "Reasonable efforts" can include advising employees of the existence of a trade secret, limiting access to the information on a "need to know basis," and storing the information on a computer database accessible only by a special password.

Examples of Trade Secrets

- BUSINESS METHODS
- SOURCE (AND, IN SOME CASES, OBJECT) CODE
- CLIENT OR CUSTOMER LISTS
- STRATEGIC PLANS
- MARKETING PLANS
- PRICING STRATEGIES
- TECHNICAL INFORMATION
- RECORDS OF ORIGINAL RESEARCH
- LABORATORY NOTEBOOKS
- INTERNAL REPORTS
- MANUFACTURING PROCESSES AND RECIPES
- MANUFACTURING FORMULAS
- RISK ASSESSMENTS
- STANDARD OPERATING PROCEDURES
- INFORMATION CONTAINED IN PROPRIETARY HARDWARE OR SOFTWARE DEPLOYED ON SITE, OR DISCERNIBLE FROM OBSERVING ACTIVITIES ON SITE

Protecting Trade Secrets Overseas: ITC

Protection of trade secrets abroad can be challenging, particularly in China and the developing world.

One option is to bring a complaint for misappropriation under U.S. Section 337 of the Tariff Act of 1930,19 U.S.C. §1337 and the U.S. International Trade Commission (ITC).

- This is only available where the misappropriation involves articles imported to the U.S., and
- Where there is injury or threat of injury to an industry in the United States

Section 337 and ITC

The following summary shows the high success rate of complainants in recent trade secrets actions at the ITC:

Investigation	ALJ	Basis of Violation	Outcome of Trade Secret Claims
DC-DC Controllers and Products Containing the Same, Inv. No. 337-TA-698	Shaw (previously Bullock, Luckern)	Patent infringement, trade secret misappropriation	Consent order and settlement agreement. Violation of consent order found in subsequent enforcement proceeding.
Electric Fireplaces, Components Thereof, Manuals for Same, Certain Processes for Manufacturing or Relating to Same and Certain Products Containing Same, Inv. No. 337-TA-791/826	Shaw (previously Gildea)	Copyright infringement, trade secret misappropriation, breach of contract, tortious inference with contract	Violation found based on default for foreign respondents. Commission issues a 5-year limited exclusion order ("LEO"). Consent order and settlement agreement with domestic respondent.
Rubber Resins and Processes for Manufacturing Same, Inv. No. 337-TA-849	Lord (previously Bullock, Rogers)	Trade secret misappropriation	Violation found. Commission issues a 10-year LEO. Fed. Cir. confirmed. Cert. denied at the Supreme Court challenging ITC's authority to adjudicated trade secrets cases
Paper Shredders, Certain Processes for Manufacturing or Relating to Same, Inv. No. 337-TA-863	Pender	Patent infringement, trade secret misappropriation	Consent order and settlement agreement with corporate respondents. Withdrawal of complaint as to individual respondents.

Section 337 and ITC

Investigation	ALJ	Basis of Violation	Outcome of Trade Secret Claims
Opaque Polymers, Inv. No. 337-TA-883	Pender	Patent infringement, trade secret misappropriation	Violation found based on sanctions for spoliation of evidence. Commission issues 25-year LEO and holds respondent and counsel joint and severally liable for almost $2 million of the complainant's costs and attorneys' fees.
Crawler Cranes and Components Thereof, Inv. No. 337-TA-887	Shaw	Patent infringement, trade secret misappropriation	Violation found. Commission issues 10-year LEO and cease and desist order.
Stainless Steel Products, Certain Processes for Manufacturing or Relating to Same, and Certain Products Containing Same, Inv. No. 337-TA-933	Essex	Trade secret misappropriation	Violation found. Commission issues a 16.7 year LEO and cease and desist order.
Certain Carbon and Alloy Steel Products, Inv. No. 337-TA-1002	Lord	Trade secret misappropriation	Sanctions issued to Chinese respondents. Terminated after finding no violation.
Certain Peridontal Laser Devices, Inv. No. 1070	Pender	Trade secret misappropriation, breach of contract, false advertising	Investigation instituted in September. Terminated after withdrawal of Complaint.

ITC Remedies for Trade Secret Misappropriation

EXCLUSION ORDERS

- **Limited**: Bar imports from an **identified source**
  - Most common
- **General:** Bar imports from **all sources**
  - Less common and difficult to get
  - Maker need not be a respondent in investigation
  - Only available if source of goods difficult to identify or if necessary to give effective remedy

CEASE AND DESIST ORDERS

- Bar entity from engaging in infringing activity related to imported article within U.S. (inventory)
- Penalty for violation of **up to $100,000** per day

ITC's Extraterritorial Authority over Trade Secrets

In *Tian Rui Group v. ITC*, 661 F.3d 1322 (Fed. Cir. 2011), the Federal Circuit held that the ITC had authority over misappropriation of trade secrets occurring entirely in China.

Facts:

- A U.S. manufacturer of railway wheels, Amsted, developed a proprietary process and licensed it to Chinese foundries
- Amsted's Chinese competitor hired employees from Amsted's Chinese foundries, who disclosed Amsted's trade secrets to Tian Rui
- After finding Tian Rui misappropriated Amsted's trade secrets in China, the ITC issued a limited exclusion order barring sales of Tian Rui's railway products in U.S.

Important lessons from *Tian Rui*

- The court **rejected the argument by Tian Rui** that, under the presumption against extraterritorial application of U.S. law, the ITC had no jurisdiction because the misappropriation occurred entirely in China. 661 F.3d at 1329
- The court held that **the ITC had jurisdiction** because the foreign "unfair" activity resulted in *importation of articles* causing injury to a domestic industry. *Id.*
- The court held that **a U.S. industry was injured** even though Amsted no longer used the trade secret process in its U.S. manufacturing
- The ITC had applied Illinois trade secrets law, but the Federal Circuit held that because Section 337 was a federal trade law, **federal common law applied**. 661 F.3d at 1327
  - Because trade secrets law "varies little from state to state," the court held that this did not affect the outcome. *Id.*

Substantive Element No. 1: Importation

- Defined as **"bringing of goods within the jurisdictional limits of the United States with the intention to unlade them"**
  - Prohibition on importation also includes a "sale for importation"
  - "Sale for importation" includes a contract for the sale of goods to be delivered at a future date, even without actual performance of the contract or importation. *Enercon GmbH v. ITC,* 51 F.3d 1376, 1381-83 (Fed. Cir. 1998)
- Although not heavily contested in most cases, "importation" was an issue in *Crawler Cranes*
  - Sany Heavy Industry Co. Ltd. ("Sany"), a Chinese heavy machinery manufacturing company, was accused of misappropriating the trade secrets of Wisconsin-based Manitowoc Cranes ("Manitowoc")
  - Among its defenses, Sany argued that the accused product was not imported or sold for importation because it had yet to be constructed
  - Based on *Enercon GmbH v. ITC*, the Commission found that because Sany had entered into a contract for the sale of the accused product, it had been "sold for importation"

Substantive Element No. 2: Existence of a Protectable Trade Secret

Four criteria for establishing trade secret misappropriation:

1. The existence of a trade secret which is not in the public domain;

2. The complainant is the owner of, or possesses a proprietary interest in, the trade secret;

3. The complainant disclosed the trade secret to respondent while in a confidential business relationship or that respondent wrongfully took the trade secret by unfair means; and

4. The respondent has used or disclosed the trade secret, causing injury to complainant.

Sausage Casings, Initial Determination at 245 (Jul. 31, 1984).

Substantive Element No. 2: Existence of a Protectable Trade Secret (cont.)

- Six (6) factors to aid in determining whether a trade secret exists:
  1. the extent to which the information is known outside of complainant's business;
  2. the extent to which it is known by employees and others involved in complainant's business;
  3. the extent of measures taken by complainant to guard the secrecy of the information;
  4. **the value of the information to complainant and to his competitors;**
  5. **the amount of effort or money expended by complainant in developing the information;**
  6. the ease or difficulty with which the information could be properly acquired or duplicated by others.

Sausage Casings, Initial Determination at 245-46 (Jul. 1984) (citing The Restatement of the Law of Torts § 757, Comment b (1939))

Substantive Element No. 2: Existence of a Protectable Trade Secret (cont.)

- In *Crawler Cranes*, Sany was accused of misappropriating trade secrets that included Manitowoc's marketing and business plans for certain crawler cranes, cost and pricing information, manufacturing process and procedures, and engineering design standards and plans.
- The Commission first rejected Sany's argument that the alleged trade secrets were not protectable because they were generally known ideas without value, for example:
  - With respect to a business trade secret regarding pricing, the Commission found that "Manitowoc spends a substantial amount of time and resources setting its dealer discount prices . . . [and] determines the cost and pricing information on a model-by-model basis."
  - Similarly, the Commission found that "Manitowoc's [technical trade secrets] for processing large weldments are valuable because they are important to the quality of the crane and they took many years to develop."

Substantive Element No. 2:
Existence of a Protectable Trade Secret (cont.)

- The Commission in *Crawler Cranes* also determined that Manitowoc took appropriate steps **to preserve the confidentiality of its secrets,** such as:
  - having employees sign confidentiality agreements
  - marking documents with sensitive information as "confidential"
  - securing access to Manitowoc's computer system
  - limited outside dissemination only to certain customers

Substantive Element No. 3: Wrongfully Taking by Improper Means

- In *Crawler Cranes*, Manitowoc's trade secrets were not taken directly by Sany, but by an employee of Manitowoc (John Lanning) who then improperly disclosed the secrets to Sany
- The Commission found Sany liable under well-established principles of agency law
  - Mr. Lanning's actions were imputed to Sany because ***Sany knew that the secrets were "improperly obtained***, specifically [by] the breach in Mr. Lanning's confidentiality obligations."
  - "[W]ith respect to acquisition by improper means, ***the driving force behind Sany's hiring of Mr. Lanning was his knowledge of Manitowoc's trade secrets***."

Substantive Element No. 4: Existing of/Injury to Domestic U.S. Industry

A Complainant may satisfy the domestic industry requirement for a trade secret misappropriation claim by establishing either that:

The domestic industry that is the "target" of the trade secret misappropriation exists and is actually or threatened to be "destroy[ed] or substantially injure[d]" by the trade secret misappropriation; or

The "establishment" of such a domestic industry has been "prevent[ed]" by the trade secret misappropriation.

Cast Steel Railway Wheels at *67 ("injury or destruction"); *Certain Caulking Guns*, Inv. No. 337-TA-139, Initial Determination, 1983 WL 207157 at *26 (Nov. 25, 1983) ("prevention of establishment").

Substantive Element No. 4: Existing of/Injury to Domestic U.S. Industry (cont.)

- *Rubber Resins* (Inv. No. 337-TA-849)
  - ALJ laid out a number of evidentiary factors used to determine whether a respondent's unfair acts have the threat or effect of substantially injuring a domestic industry

Actual Injury	Threat of Injury
(1) the respondent's volume of imports and penetration into the market; (2) the complainant's lost sales; (3) underselling by the respondent; (4) the complainant's declining production, profitability and sales; and (5) the harm to complainant's goodwill and reputation	(1) substantial foreign manufacturing capacity; (2) ability of imported product to undersell the domestic product; (3) explicit intention to enter into the U.S. market; (4) the inability of the domestic industry to compete with the foreign products because of vastly lower foreign costs of production and lower prices; and (5) the significant negative impact this would have on the domestic industry

Substantive Element No. 4:
Existing of/Injury to Domestic U.S. Industry (cont.)

Evidence Demonstrating an Injury to a Developed Domestic Industry

- Volume of imports and their degree of penetration
- Lost sales/profits
- Underselling by respondents
- Reduction in complainants' profits or employment levels
- Declining production, profitability and sales

Certain Electric Power Tools, Battery Cartridges, and Battery Chargers Contents, Inv. No. 337-TA-284, Comm'n Determination, 1990 WL 710470 at *123 (Feb. 20, 1990).

Evidence Demonstrating an Injury to a Nascent or Embryonic Domestic Industry

- Foreign cost advantages and production capacity
- Ability of the imported product to undersell the domestic product
- Substantial foreign manufacturing capacity combined with the Respondent's intention to penetrate the U.S. market

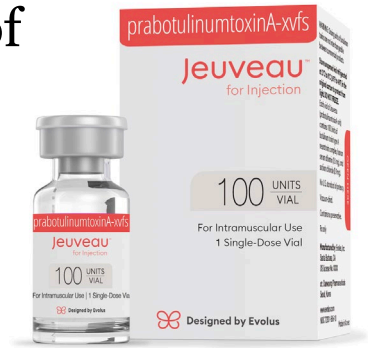
Electric Power Tools, at *124. See also, *Certain Air Impact Wrenches*, Inv. No. 337-TA-311, Initial Determination at *65 (May 6, 1991).

Substantive Element No. 4: Existing of/Injury to Domestic U.S. Industry (cont.)

- In *Crawler Cranes*, the Commission found that Sany's misappropriation of trade secrets injured Manitowoc's domestic industry in many ways, for example:
  - "Sany's misappropriation caused injury to Manitowoc's domestic industry [because] Manitowoc's welding procedures guided Sany in its development of the [its] SCC8500 crane"
  - "Sany's use of Trade Secret No. 14 injured Manitowoc's domestic industry for 400-600 ton crawler cranes because Sany was able to target its pricing at the Manitowoc 16000 crane" (lowering Manitowoc's profit margins)

Case Example: Botox (337-TA-1145)

- South Korean company Medytox and its affiliates brought a complaint against South Korean company Daewoong and U.S.-based licensee Evolus over misappropriation of trade secrets relating to Botox bacteria and methods of manufacturing.
  - The misappropriation occurred entirely abroad (South Korea).
  - Medytox and its affiliates did not themselves practice the trade secrets.



- Yet, the ITC issued a Limited Exclusion Order, prohibiting importation of Daewoong and Evolus Botox products for 21 months.
  - The Commission rejected the ALJ's recommendation of a 10-year ban.
  - ITC also issued a cease and desist order against Evolus, preventing sale, marketing, or promotion of Daewoong and Evolus Botox products for 21 months.
- Daewoong and Evolus appealed to the Federal Circuit.

Determining the Length of Remedy

- For patent infringement: the duration of the term of the patent. *Texas Instruments Inc. v. United States Int'l Trade Comm'n*, 851 F.2d 342, 344 (Fed. Cir. 1988).
- For trade secret misappropriation: the **"reasonable research and development period"** or **"independent development time"** that would be required to reproduce the trade secrets by lawful means. *See Certain Apparatus for the Continuous Production of Copper Rod*, Inv. No. 337-TA-52, Comm'n Op. at 67 (Nov. 1979); *Sausage Casings*, Comm'n Decision at 19 (Dec. 1984).

Case Example: Foreign Theft of Biotech

THE UNITED STATES DEPARTMENT of JUSTICE

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Monday, February 1, 2021

Hospital Researcher Sentenced to Prison for Conspiring to Steal Trade Secrets, Sell Them in China

- Ohio researcher Li Chen took trade secrets relating to exosome research from the Nationwide Children's Hospital Research Institute in Columbus, Ohio.
- Chen started a company in China to sell exosome "isolation kits"
- Chen received benefits from the Chinese government for biotech research
- Chen and her husband pled guilty to Trade Secret theft
- Chen sentenced to 30 months; fined $2.6 million

Practice Pointers

- **Think about how to define your trade secrets early (broad to narrow), and how to describe them in a public complaint.**
  - What did defendant have access to?
  - What might have been incorporated into a competing product?

- **Be aware of all ways your information is being disseminated.** (Do you teach courses to partners? Have tech support blogs? Youtube channels? Give detailed presentations at trade shows?) Identify ways your TS could have been disclosed before defendant does

- **Know your patents and what you disclosed to the copyright office.**

- **Think about damages.** Even if you can't prove trade secrets were actually incorporated into a product, courts have accepted "avoided costs" models – your trade secrets taught them what NOT to do

Practice Pointers (cont.)

- **Think about other claims and how they will affect your case.**
  - Breach of contract and other business torts may be preempted
  - Bringing breach of contract claims may subject you to unfavorable terms under the contract (choice of law, forum selection, damages limitations)
  - Patent and trade secret claims are rarely brought together because of the disclosure tension

- **Before filing, consider whether you will need to move for TRO, seek ex parte seizure of misappropriated TS, or seek a preservation order to prevent spoliation of evidence by defendant.**

- **Consider trade secrets action at the ITC.**
  - Can cover foreign conduct
  - Faster adjudication (typically 16 months to final judgment)
  - District courts have given ITC DTSA holdings preclusive effect

Any questions? Please contact

Mark L. Whitaker

Partner, Washington D.C.
(202) 887-1507
mwhitaker@mofo.com

Mark Whitaker is co-chair of the firm's global IP Litigation Practice and cross-disciplinary Intellectual Property Group. Mark's clients benefit from his more than 30 years of experience crafting litigation strategies in high-stakes patent and trade secret litigation. Mark sees the whole board for each of his clients, and works closely with them to define a successful litigation outcome, and determine the best path to achieve that goal. He has extensive experience navigating the rules and procedures in the nation's top patent litigation venues, including U.S. district courts, the International Trade Commission, and the Court of Federal Claims.

Mark regularly acts as lead counsel in matters involving technologies such as semiconductors, photo/optical technologies, chemicals, and database analytics. His clients do business in a broad range of industries including pharmaceuticals, medical devices, consumer products, and telecommunications. He often leads a team of MoFo lawyers representing several defendants in parallel multipatent litigations.

Full bio available here.

APPENDIX

- Pre-DTSA TS Litigation
- Additional Trade Secret Considerations

Litigation: Pre-DTSA

STATE LAWS

- 48 of 50 states have adopted some version of the UTSA (including Massachusetts)
- Restatements of Torts & Unfair Competition
- Main differences among state laws:
  - Inevitable disclosure
  - Non-competes
  - Methods of damages calculation
  - Statute of limitations

FEDERAL LAWS

- Economic Espionage Act
- Computer Fraud and Abuse Act
- ITC Section 337

Example of Non-Compete Agreement

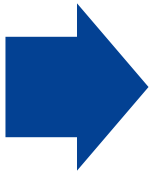
Non-Competition Agreement prohibits former sandwich artists, delivery drivers, and other employees from working at food service venues within 3 miles that derive 10% or more of their revenue from the sale of sandwiches, submarines, or wraps for two years following employment

Litigation: DTSA Overview

- Enacted May 11, 2016
- Around 1,400 federal trade secret cases are filed annually, up from 1,100 pre-DTSA
- Most popular jurisdictions are N.D. Ill., N.D. Cal., C.D. Cal., S.D.N.Y., and E.D.P.A.

ADDRESSED

- Jurisdiction
- Trade secret definition
- Seizure
- Whistleblowers
- Preemption of state trade secrets laws



NOT ADDRESSED

- Inevitable Disclosure
- Enforceability of non-competes
- Preemption of other state law claims
- Identification of trade secrets
- International aspects

DTSA: Quick Facts

FIGURE 4:
Case Activity by Industry Sector

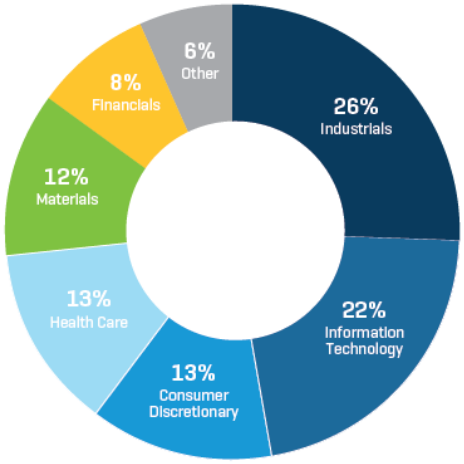
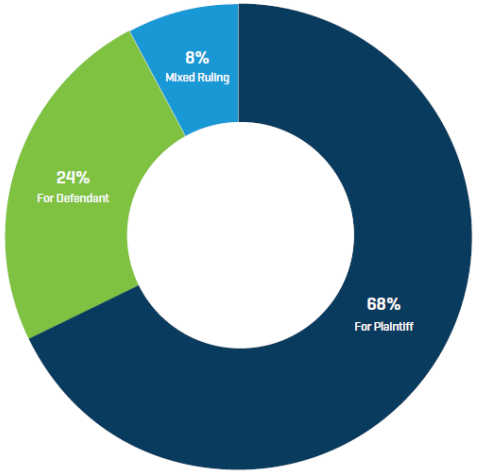


FIGURE 13:
Proportion of Court Rulings by Prevailing Party*



*This figure excludes cases resulting in a settlement.

FIGURE 7:
15 Most Active District Courts (Trade Secret Decisions)

DISTRICT COURT		CIRCUIT	NO. OF CASES	% OF TOTAL
Northern District of Illinois		7th	20	7.8%
Eastern District of Texas		5th	20	7.8%
District of Colorado		10th	17	6.6%
District of Massachusetts		1st	15	5.8%
Northern District of Texas		5th	11	4.3%
Southern District of Florida		11th	11	4.3%
Western District of Texas		5th	11	4.3%
Northern District of California		9th	9	3.5%
Eastern District of Pennsylvania		3rd	7	2.7%
Southern District of Texas		5th	6	2.3%
Southern District of California		9th	6	2.3%
Southern District of Iowa		8th	6	2.3%
Eastern District of Michigan		6th	6	2.3%
District of Minnesota		8th	6	2.3%
District of New Jersey		3rd	6	2.3%
All Other Districts			100	38.3%
Total Cases			257	

Source: Trends in Trade Secret Litigation Report 2020, Stork LLC

Case Law: Use Required Post-DTSA

- Courts have clarified that a DTSA cause of action may be based on a misappropriation that occurred ***prior to*** DTSA's effective date

- But ***only if*** the unauthorized use of the trade secrets continued after the DTSA effective date

- E.g. *Syntel Sterling Shores Mauritius Limited v Trizetto Group* (SDNY)
  - Any post-enactment use is sufficient to support DTSA jurisdiction even if the wrongful misappropriation occurred prior to enactment

Remedies and Limitations

INJUNCTIONS

- Available to prevent actual or threatened misappropriation
- Order may not "prevent a person from entering into an employment relationship, and that conditions placed on such employment shall be based on evidence of threatened misappropriation and not merely on the information the person knows"
- The order also may not otherwise conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business

LIMITATIONS

- Must be filed within 3 years after the misappropriation is discovered

Damages

DAMAGES

- Actual loss; and
- Unjust enrichment that is not addressed in computing damages for actual loss
- In lieu of other damages, a reasonable royalty
- Enhanced damages, up to 2X, if trade secret is willfully and maliciously misappropriated

ATTORNEY'S FEES

- If trade secret is willfully misappropriated
- If claim of misappropriation is made in bad faith

Whistleblower Protection

IMMUNITY

- An individual shall not be held criminally or civilly liable under any Federal or State trade secret law for the disclosure of a trade secret that
  - **(A)** is made–
    - (i) in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney; and
    - (ii) solely for the purpose of reporting or investigating a suspected violation of law; or
  - **(B)** is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal

Notice Requirement

- Required in any contract or agreement with an employee (defined to include contractors)
- May be satisfied by specific language, or cross-reference to policy document
- Penalty is no exemplary damages and attorneys fees

US Case Example: *Teradata v. SAP*

- Teradata and SAP entered partnership to connect Teradata's database analytics with SAP's enterprise software (with NDA and other agreements defining the project)
- After three years of joint work, SAP terminates partnership, announces its own database analytics offering the following month
- Teradata does not initially suspect foul play, learns of misappropriation via an article in *Der Spiegel* four years later
- SAP's new product was not as successful as SAP hoped, so SAP has started forcing customers to upgrade and adopt it
- Case filed in ND Cal with trade secret (DTSA and CUTSA), copyright, and antitrust claims; case set for trial in 2021

Case Example: *Foreign Theft of Biotech*

THE UNITED STATES DEPARTMENT of JUSTICE

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Monday, February 1, 2021

Hospital Researcher Sentenced to Prison for Conspiring to Steal Trade Secrets, Sell Them in China

- Ohio researcher Li Chen took trade secrets relating to exosome research from the Nationwide Children's Hospital Research Institute in Columbus, Ohio.
- Chen started a company in China to sell exosome "isolation kits"
- Chen received benefits from the Chinese government for biotech research
- Chen and her husband pled guilty to Trade Secret theft
- Chen sentenced to 30 months; fined $2.6 million

Application to Foreign Activity

DTSA APPLIES TO CONDUCT OCCURRING OUTSIDE THE UNITED STATES IF:

- (1) the offender is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof; or
- (2) an act in furtherance of the offense was committed in the United States.

Patents vs. Trade Secrets: Business Considerations

COMPARE COSTS:

- *Prosecuting patents* in key jurisdictions where intellectual property protection matters OR
- *Protecting information* within the company

CONSIDER:

- Will a patent generate licensing streams or favorable cross-license terms?
- Or is it primarily for defensive purposes – to exclude competitors?

Protecting Trade Secrets

- **Clean Exit, Clean Entry.** Misappropriation is most likely to occur when:
    - Employee begins a new job (bringing with her information from prior employer, most of the time unwittingly)

      OR

    - Employee leaves the job (taking with him information from old employer, most of the time unwittingly)

- Trade secret protection measures offered in the next few slides geared towards mitigating these "in-bound" and "out-bound" trade secret misappropriation risks

Basic Trade Secret Protection Measures

Employment Agreement and Annual Certification of Compliance	•Provisions require employees to safeguard company confidential information; also to record and disclose their inventions, and to not use others' trade secrets •Require annual certification with Corporate Compliance Policy
Procedures for departing employees	•Exit meeting with manager •Employee Departure Form including certification acknowledging obligation not to divulge proprietary information •Exit survey for voluntary separation asking for future employment plans •Review computer usage in weeks' prior to departure to detect improper conduct
Procedures for onboarding employees	•Entrance interview with manager •Employee Onboarding Form including similar certification acknowledging no possession of proprietary information from previous employers

Physical Security Measures

PROTECTION OF PERIMETER AND GROUNDS FROM UNAUTHORIZED ACCESS

AUTHORIZED ACCESS GENERALLY:

- Employees (with badge)
- Contractors (with badge, usually time-restricted)
- Visitors (with paper badge and host escort)

AUTHORIZED ACCESS TO MORE RESTRICTED BUILDINGS AND AREAS:

- Building manager authorizes access
- Area manager authorizes access to specific laboratories or clean environments within the building
- Emergency access

Virtual Security Measures

- Login requirements, firewalls, and security audits protect information on software tools, servers, desktop computing, and portable devices
- Require encryption of data sent to third parties
- Regularly run up-to-date malware/antivirus software programs
- Pay particular attention to security of web applications
- Require smarter password management

Which Brings Us to… BYOD Policies

Bring Your Own Device ("BYOD") policies are essential in this era where employees use their own devices for company work. Here are some key provisions:

- Make use of personally owned devices voluntary, giving employees the option of using a company device instead
- Impose technical security standards as a condition of network access, including encryption, remote wipe, and password protection, to ensure that the device is protected to the same level as would any other company issued device
- Make use of personally owned devices conditional on employees' consent to the company's ability to monitor, remotely wipe company data, and inspect the device at any time and for any reason
- Prohibit use of any file sharing applications while connected to the company's network or on company premises, including Snapchat, Instagram, and the like.
- Give clear notice, especially of monitoring and remote wipe functions, to avoid breach of any employee privacy laws or regulations
- Obtain a signed agreement to the BYOD policy prior to allowing any network access from a personally owned device

Create a "Culture of Data Security"

Implement a regular schedule of employee training

Regularly remind employees of company policy—and any legal requirement—to keep client information secure and confidential

Know which employees have access to sensitive information. Pay particular attention to data like Social Security numbers and account numbers. Limit access to personal information to employees with a "need to know"

Use software within the company to prevent copying, printing, and e-mailing of truly critical trade secrets

Involve functions across the company in data security (*e.g.,* Information Technology, Security, Finance, Human Resources). It is important to involve Human Resources because that function may be most knowledgeable about how employees actually are carrying out their work

Consider creating a data security committee to include all corporate functions that have a stake in these issues. Data security committees should regularly (i) audit corporate security practices, and (ii) meet to keep pace with how employees are using the latest technology

Strategy for Reviewing Specific Trade Secrets