Trends in Trade Secret Litigation

Developments in Trade Secret Litigation and Protecting Trade Secrets in Remote Work Environment

ACC Association of Corporate Counsel HOUSTON

Schlumberger

BAKER BOTTS

Speakers

Ashley Brown
Schlumberger
IP Enforcement Counsel

Paul Morico
Baker Botts
IP Partner/Firmwide
Energy IP Sector Chair

Natalie Gonzales
Baker Botts
IP Partner

Overview

Trade Secrets in 2020

Realities of COVID-19's remote work environment and impact on trade secret protection/litigation; general definitions, legal standards, and principles.

Trends in Trade Secret Litigation

Recent trends in trade secret litigation and recent development related to key considerations.

Protecting Trade Secrets in Remote Environment

Explore dangers to trade secrets in remote work environment; safeguarding trade secrets; how to handle departing employee issues.

TRADE SECRETS IN 2020

01

ACC Association of Corporate Counsel HOUSTON

Schlumberger

BAKER BOTTS

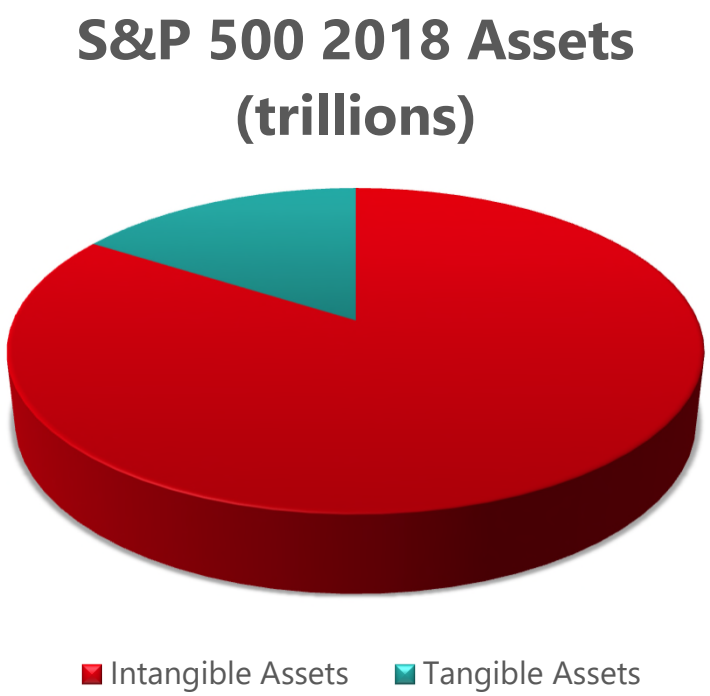
The Reality of COVID-19

- Millions of employees working at home, many on their own computers and phones

- Layoffs of employees with knowledge of trade secrets (e.g., authors and inventors) may put IP at risk

What's the big deal?

- Global Survey by Ponemon Institute & Symantec
  - 59% of Employees Leaving a Job ADMIT to Keeping Corporate Data When They Leave
  - 40% ADMIT they intend to use the information in their new job
  - 44% DO NOT believe it is a crime to use a competitor's trade secrets
- Even before the current crisis, studies estimated U.S. companies were losing $300 billion/yr from trade secret misappropriation



Trade Secrets

- Almost anything!
- More than just technology
- In fact, business trade secrets may be more valuable
- Can include what not to do or what did not work
- Subset of “confidential” information

Sources of Trade Secret Law

- Federal, State and International Legislation
  - Uniform Trade Secrets Act (UTSA)
    - All states except New York, Massachusetts, & North Carolina
  - U.S. Defend Trade Secrets Act (DTSA)
    - Signed May 11, 2016
    - Largely tracks UTSA

Trade Secret Law - UTSA

- UTSA* defines a trade secret as:
  - **Information**, such as a formula, pattern, compilation, program, device, method, technique or process, that
    - Derives independent economic value . . . from not being generally known to . . . other persons who can obtain economic value from its disclosure or use, and
    - Is the subject of efforts that are reasonable . . . to maintain its secrecy
- 3-year statue of limitations
  - Most states adopted, including Texas
  - Some rejected in favor of 2, 4, 5, or 6 year limitations periods

*Texas enacted its version of the UTSA on Sept. 1, 2013 – Chapter 134A, Texas Civil Practice and Remedies Code

Trade Secret Law – DTSA

- DTSA (18 U.S.C. Section 1836) defines a trade secret as:
  - Trade Secrets include financial, business, scientific, technical, economic, or engineering information, so long as:
    - Reasonable measures to keep the information secret have been taken
    - Information derives independent economic value from not being known by the public
- Defines remedies, including damages and injunctive relief, and allows for *ex parte* seizure of misappropriated trade secrets
  - Certain relief depends on whether employee had notice of employee immunity provision in DTSA (e.g., whistle-blower provision)
- Includes a 3-year statute of limitations

What are "Reasonable" Efforts/Measures

- Indicators of reasonable efforts (and thus, trade secrecy) include:
  - Value to trade secret owner
  - Circumstances of disclosure (to employees and to third-parties)
  - Security measures (facility, computers, documents/records, etc.)
  - Express agreements (NDAs, Confidentiality Agreements, others?)
  - Actual enforcement

- "Reasonableness" depends on nature of information being protected: generally, higher value means more effort.

TRENDS IN TRADE SECRET LITIGATION 02

ACC Association of Corporate Counsel HOUSTON

Schlumberger

BAKER BOTTS

Trade Secrets in the news…

- China's efforts to steal COVID-19 vaccine data
- fig spread
- medical marijuana state licensing applications (includes applicants' proprietary information on things like fertilizer, pesticides and cannabis processing)
- craft beer formulas
- recipes for popcorn
- methods for bleaching hair and repairing hair damage
- process of adding aromas to beverage bottles to enhance the perceived taste
- designs and manufacturing processes for drones
- design of fracking sand shipping containers

Recent Trade Secret Litigation Trends

- Trade Secret case filings increased 30% between 2015 and 2017 (due to the DTSA in 2016) and have remained steady between 2017 and 2019

Figure 1: Trade Secret Case Filings 2010 to 2019

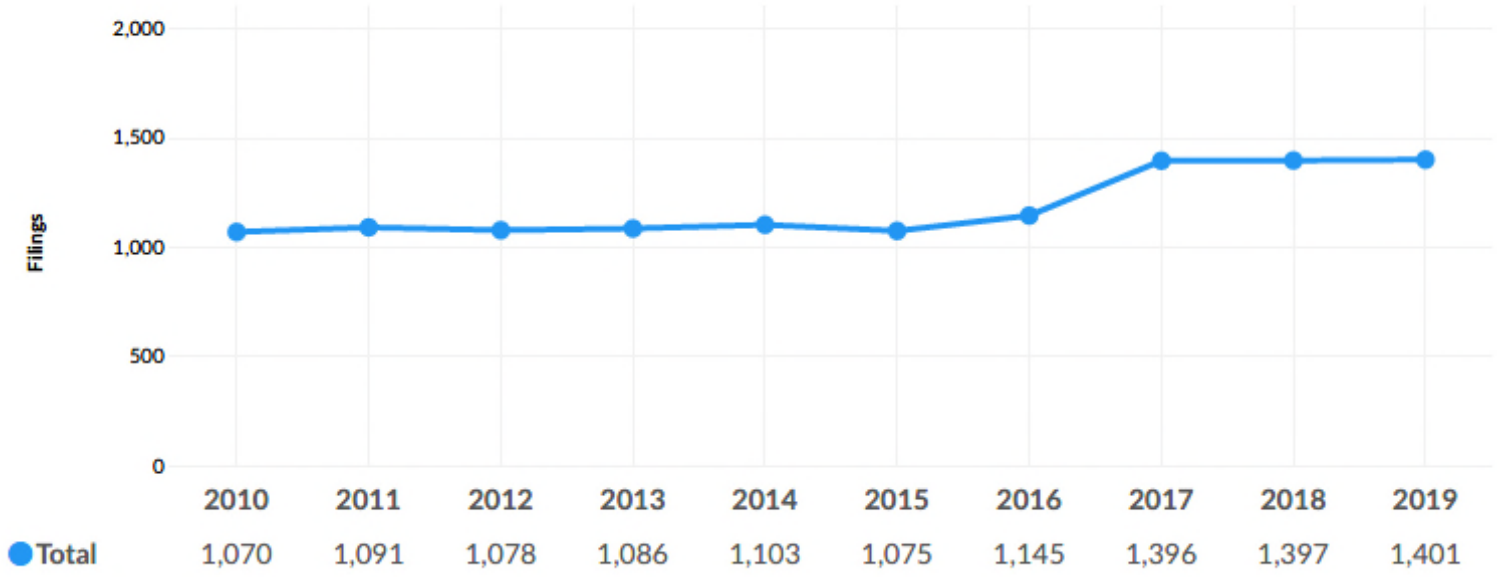


Figure from Lex Machina 2020 Trade Secret Litigation Report

Recent Trade Secret Litigation Trends

- In 2019, 72% of all Trade Secret cases in federal district court had DTSA claims and over 80% of Trade Secret cases had contract claims (breach of contract, tortious interference, etc.)

- In 2019, courts awarded damages in fewer Trade Secret cases than in 2018 but awarded a larger amount of money damages overall ($105 million in 2019 versus $71.9 million in 2018)

- Of terminated cases, 156 ended for failure to identify a trade secret; 116 were terminated for failure to maintain secrecy

Figure 20: Ownership Findings for Cases Terminated from 2010 to 2019

Findings	Default Judgment	Consent Judgment	Judgment on the Pleadings	Summary Judgment	Judgment as a Matter of Law	Trial	Any Judgment Event
Ownership / Validity	0	4	6	20	53	0	83
Failure to Identify Trade Secret	3	0	41	101	11	1	156
Failure to Maintain Secrecy	0	0	23	74	18	3	116
Generally Known / Readily Ascertainable	0	0	4	54	13	1	72
No Ownership / Validity: Wrong Entity	0	0	7	10	2	0	19

Figure from Lex Machina 2020 Trade Secret Litigation Report

Recent Trade Secret Litigation Trends

- Recent patent trends may lead to increased trade secret litigation
- Potential increase in labor and employment litigation in current environment
- Likely increase in already high percentage of trade secret cases involving current and former employees

Recent Developments Related to Key Considerations

- Identifying trade secrets with reasonable particularity
- Reasonable efforts to maintain secrecy
- Statute of limitations
- Remedies (e.g., head start damages, attorney's fees, and injunctions)
- FOIA exemption for trade secrets

What's the trade secret?

- Where and how to identify trade secrets
  - Complaint
  - Pre-discovery statement (filed under seal)
    - *See, e.g., California Code of Civil Procedure* § 2019.210 – "In any action alleging the misappropriation of a trade secret under the [California] Uniform Trade Secrets Act ... , before commencing discovery relating to the trade secret, the party alleging the misappropriation shall identify the trade secret with reasonable particularity[.]"
    - Texas does not have any timeline for required disclosure except deadline of 30 days before trial to supplement discovery
  - Interrogatory response

Identifying Trade Secrets with Reasonable Particularity – Not Sufficient

- *Waymo, LLC v. Uber Technologies, Inc.*, No. 17-00939, 2017 WL 6887040, *7-9 (N.D. Cal. Nov. 14, 2017) (ref Oct. 30 decision)
  - Section 2019.210 of the California Code of Civil Procedure: trade secrets to be identified "with reasonable particularity" prior to discovery
  - Schematic as well as "strategies or concepts reflected in the schematic" and "unique and unknown design characteristics such as the selection and layout of individual electrical components, and the required manufacturing tolerances.
  - Waymo's disclosure "came nowhere near the required reasonable particularity"

- *U.S. v. Anthony Levandowski*, No. 3:19-cr-00377 (N.D. Cal. 2019)
  - Levandowski moved for Bill of Particulars re specificity with which trade secrets were identified after Judge Alsup raised the issue during a status conference
  - Parties agreed that the trade secret was each file in its entirety

Identifying Trade Secrets with Reasonable Particularity – Not Sufficient

- *Zoom Imaging Solutions, Inc. v. Roe*, No. 2:19-cv-1544, 2019 WL 5862594 (E.D. Cal. Nov. 8, 2019)
  - No identification of its trade secrets in complaint other than list of Confidential Information and referring to "business information" and "valuable information"

- *AlterG Inc. v. Boost Treadmills LLC*, No. 18-cv-7568, 2019 WL 4221599 (N.D. Cal. Sept. 5, 2019)
  - "not readily apparently what material differences" there were and "technical matters . . . are more complex to begin with and therefore warrant greater specificity"

Identifying Trade Secrets with Reasonable Particularity - Sufficient

- *Yeiser Research & Dev., LLC v. Teknor Apex Co.*, No. 17-CV-1290-BAS-MSB, 2019 WL 2177658 (S.D. Cal. May 20, 2019)
  - Technology not so complicated (garden hose)
  - Plaintiff's interrogatory response found to be sufficient during discovery

- *WeRide Corp. v. Kun Huang*, 379 F. Supp. 3d 834, 845 (N.D. Cal. 2019)
  - WeRide described the functionality of each trade secret; named numerous files in its code base that reflect the source code specific to each alleged trade secret
  - WeRide "need not spell out the details" of the alleged trade secrets; instead must provide sufficient identification so court and defendant may "ascertain at least the boundaries within which the secret lies"

Identifying Trade Secrets with Reasonable Particularity - Sufficient

- *GlobeRanger Corp. v. Software AG United States of America, Inc.*, 836 F.3d 477, 492 (5th Cir. 2016)
  - "Texas law does not require great detail in the definition of a trade secret."

- *Vianet Group PLC v. Tap Acquisition, Inc.*, No. 3:14-cv-3601, 2016 WL 4368302, at *20 (N.D. Tex. Aug. 16, 2016)
  - Finding it sufficient for the plaintiff to "identify specific groupings of information that contain trade secrets, identify the types of trade secrets contained in the groupings, and explain how the alleged trade secrets were maintained and treated as secrets"

- *A&P Tech., Inc. v. Lariviere*, No. 1:17-CV-534, 2017 WL 6606961, at *8 (S.D. Ohio Dec. 27, 2017)
  - Divergent rulings from federal courts "reinforces the idea that rulings on discovery limitations are a case-by-case decision where courts must use their broad discretion based heavily on the distinct circumstances of any particular action"

Failure to Maintain Secrecy – What not to do

- *Yellowfin Yachts, Inc. v. Barker Boatworks, LLC*, 898 F.3d 1279 (11th Cir. 2018)
  - Plaintiff failed to instruct defendant to secure company information on his personal devices, allowed the defendant to access information after he refused to sign a confidentiality agreement, and failed to mark information as confidential

- *Temurian v. Piccolo*, No. 18-cv-62737, 2019 WL 1763022, at *11 (S.D. Fla. April 22, 2019)
  - Plaintiff gave Defendants temporary access to alleged confidential information and trade secrets to develop back office software system (later password protected and visible to only plaintiff's officers), without any confidentiality agreement

- *Abrasic 90 Inc. v. Weldcote Metals, Inc.*, 364 F.Supp.3d 888, 898-99 (N.D. Ill. Mar. 4, 2019)
  - Plaintiff had no NDAs, no instructions to employees that info was confidential, no confidential label on documents or password protection, did not ask employees upon departure if they possessed confidential info or ask for return/deletion of documents

Adequate Measures for Maintaining Secrecy

- *WeRide Corp. v. Kun Huang*, 379 F. Supp. 3d 834, 845 (N.D. Cal. 2019)
  - Plaintiff restricted offsite access to source code, encrypted the code, and required employees to sign confidentiality agreement

- *Southern Field Maint. & Fabrication LLC v. Killough*, No. 2:18-cv-581-GMB, 2019 WL 360515, at *4 (M.D. Ala. Jan. 29, 2019)
  - Plaintiff did not mark the document at issue as "confidential"
  - "under all the circumstances, if the employee knows or has reason to know that the owner intends or expects the information to be secret, confidentiality measures are sufficient"

- *Zoppas Indus. De Mexico, S.A. de C.V. v. Backer EHP Inc.*, 2019 WL 6615421 at *3 (D. Del. Dec. 5, 2019)
  - NDA between parties, plus plaintiff continued to request that Defendant "either return or destroy [the] information" after relationship soured

Statute of Limitations

- *CMI Roadbuilding, Inc. v. Iowa Parts, Inc.*, 920 F.3d 560 (8th Cir. 2019)
  - CMI knew its component part technology was being utilized by Iowa Parts as early as 2002 (sent a warning letter to former employee)
  - Suit filed in 2016 when Iowa raised its prices
  - "At the point [plaintiff] was on notice there was a possible problem, it had a duty to investigate, regardless of its exact knowledge."

- *Alta Devices, Inc. v. LG Electronics, Inc.*, No. 18-cv-404, 2019 WL 1924992, at *14 (N.D. Cal. Apr. 30, 2019)
  - LGE's failure to return documents (as required by NDA) placed Alta on "inquiry notice" of misappropriation, which started the three year limitations period

Remedies for Trade Secret Misappropriation

- Monetary Remedies:
  - Actual losses (lost profits)
  - Unjust enrichment (if not duplicative of lost profits)
  - Reasonable royalty / ongoing reasonably royalty in certain circumstances
  - Treble damages and fees for willful/malicious misappropriation

- Equitable Remedies:
  - Temporary Restraining Orders (~68% grant rate)
  - Preliminary Injunction (~55% grant rate)
  - Permanent Injunction (~80% grant rate)

- *Ex Parte* Seizure Request – requires extraordinary circumstances

"Head Start" Damages & Attorney's Fees

- *Sabre GLBL, Inc. v. Shan*, 779 Fed. App'x 843 (3d Cir. 2019)
  - Sabre's employee started a competing Chinese company during her employment
  - Sabre pursued "head start" damages that quantified Shan's unjust enrichment:
    - Shan's company was 2 years further along in its development and commercialization than it would have been absent her use of Sabre's confidential information and trade secrets
  - Third Circuit affirmed an arbitrator's award of $1.1 million in "head start" damages

- *Orbison v. Ma-Tex Rope Company, Inc.*, 553 S.W.3d 17 (Tex. App. – Texarkana 2018)
  - District court awarded $2,000 in lost profits, $120,000 for lost good will, and $4,000 as unjust enrichment; also awarded $216,000 in attorney's fees
  - Court of Appeals found evidence was legally insufficient for all but the $4,000 unjust enrichment damages, but did not disturb the $216,000 fee award

Injunctive Relief

- What are the key factors in obtaining a preliminary injunction
  - Generally the same as in a state-law case
    - Likelihood of success on the merits
    - Irreparable harm if status quo is not maintained
    - Balancing of public and private interest factors favors injunctive relief
- Expedited relief in the form of temporary restraining orders and preliminary injunctions decreased in 2019 –
  - Court unable to determine if there was a trade secret
  - Evidence the defendant gave back all materials
- Plaintiffs need to provide the requisite specificity to show the court a trade secret exists

FOIA's Exemption

- *Food Marketing Institute v. Argus Leader Media,* 139 S.Ct. 2356, 2366 (2019)
  - Argus filed a FOIA request for data collected by the US Department of Agriculture which retailers report to the USDA but do not publicly disclose
  - Lower courts ordered release of the information finding disclosure would not cause substantial competitive harm to participating retailers
  - SCOTUS reversed:
    - Commercial or financial information treated as private by its owner and provided to the government under assurance of privacy is shielded from disclosure

PROTECTING TRADE SECRETS IN REMOTE ENVIRONMENT

03

ACC Association of Corporate Counsel HOUSTON

Schlumberger

BAKER BOTTS

Dangers to Trade Secrets with Work at Home

- Unsupervised employees might more easily copy data
- Employees may be using their own computers/phones without standard security measures
- Systems employed in a rush to facilitate work at home may have security flaws
    - E.g. Zoom

Common Methods Used for IP Theft

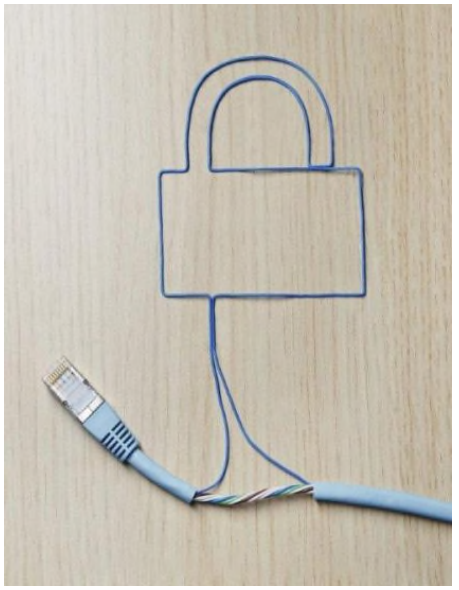
- Copy files to USB or hard drive
- Burn files to CD/DVD
- Email files to personal e-mail account
- Upload files to cloud storage service (OneDrive, Dropbox, Google Drive, etc.)

Measures to Implement

- Be sure employees are bound by a confidentiality agreement or policy
- Provide written reminders / warnings to employees regarding confidentiality while working at home
- Create a personal device usage policy (also known as a BYOD Policy—bring your own device)

Clearly Identify Confidential and Trade Secret Information / Policies / Trainings

- Should always have a written BYOD policy
- Key considerations for BYOD policies:
  - Technological Approach
  - Authorized Use/Employee Responsibilities
  - Device Security Requirements
  - On- and Off-boarding Procedures
  - Ongoing Education on the Policy
  - Ongoing Review of the Policy
  - Actual Enforcement of the Policy



- Other policies – computer use, cybersecurity, social media, etc.
- Trainings on classification of proprietary information and permissible uses of proprietary information

Implement Additional Measures if Needed

- Monitor copying/downloading of data and company files
- Remote wiping/inspection capability
- Anti-virus, malware, spyware software

Red Flags

- Only a few files on device
- Missing e-mail
- Programs recently uninstalled
- Recent e-mails to personal account
- Evidence of forensic programs used to delete information
- Evidence of cloud-based remote storage services
- Transfer of large amount of files from network to local hard drive / USB drive

Employee is Leaving . . . Now what?

- Conduct exit interview and retrieve devices / company information
- Preserve evidence and maintain chain of custody
- Forensic Evidence
- Utilize Tex. R. Civ. P. 202

Questions?

Ashley Brown
Schlumberger
IP Enforcement Counsel

Paul Morico
Baker Botts
IP Partner, Firmwide Energy IP Sector Chair
paul.morico@bakerbotts.com

Natalie Gonzales
Baker Botts
IP Partner
natalie.gonzales@bakerbotts.com

AUSTIN

BEIJING

BRUSSELS

DALLAS

DUBAI

HONG KONG

HOUSTON

LONDON

MOSCOW

NEW YORK

PALO ALTO

RIYADH

SAN FRANCISCO

WASHINGTON

bakerbotts.com