Avoiding (or winning) Trade Secret Disputes: Best Practices for Employers and Employees

Presented by

Wesley G. Lotz

Fulkerson Lotz LLP

December 12, 2018

KEY QUESTIONS

- Why are trade secrets disputes so common?
- What are the best practices for the employer to protect trade secrets and prevent trade secret theft?
- What are the best practices for a departing employee to avoid claims of misappropriation?

A Billion Dollar Problem

"Publicly traded U.S. companies own an estimated **$5 trillion worth of trade secrets**."
https:/fas.org/sgp/crs/secrecy/R43714.pdf (U.S. Chamber of Commerce)

"The Commission on the Theft of American Intellectual Property estimates that the theft of trade secrets costs the U.S. economy **$300 billion a year**".
http://www.ipcommission.org/report/ip_commission_report_052213.pdf

"A recent study by PricewaterhouseCoopers … suggests that the economic loss attributable to trade secret theft is between **1% to 3% of U.S. Gross Domestic Product**."
https:/fas.org/sgp/crs/secrecy/R43714.pdf

"Economists estimate that trade secrets comprise roughly **two-thirds of the value of companies' intellectual property** portfolios and reflect a key competitive advantage."
http://www.willamette.com/insights_journal/16/spring_2016_11.pdf

WHO IS TAKING TRADE SECRETS?

"Half of employees who left or lost their jobs in the last 12 months kept confidential corporate data, according to a global survey from Symantec (Nasdaq: SYMC), and 40 percent plan to use it in their new jobs."

https://www.symantec.com/about/newsroom/press-releases/2013/symantec_0206_01

"Another survey has estimated that 79 percent of employees in positions like finance, sales, and marketing misappropriate data when they leave employment…"

https://www.bizjournals.com/dallas/news/2016/12/21/texas-in-the-top-5-for-trade-secret-litigation.html

"More than 85 percent of misappropriation cases are estimated to involve a trade secret owner's employee or business partner, according to a 2016 study by economic and financial consulting firm Cornerstone Research."

https://www.skadden.com/insights/publications/2018/01/2018-insights/the-rise-of-trade-secret-litigation

How Data Is Being Stolen

The Symantec study (2013) found that of the 50 percent who admitted taking company files:

53 percent of employees stole data by **downloading it to a CD or DVD**.

42 percent stole data by connecting a **thumb drive** to a computer

38 percent transferred data to a **personal e-mail account**.

The most commonly information: **e-mail lists, employee records, and customer information.**

24 percent of employees still had **access to the company's computer network after leaving the company**. 20 percent still had network access more than a week after employment ended. https://www.symantec.com/about/newsroom/press-releases/2013

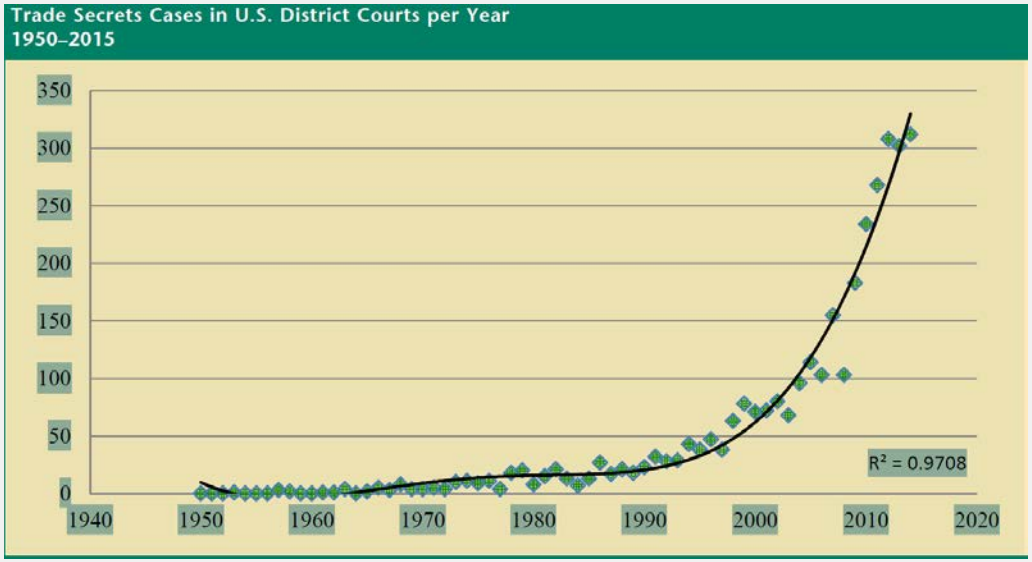
"The results show that a staggering **72 percent** of employees are willing to share sensitive, confidential or regulated company information … more than one in three employees (**35 percent)** say it's common to take corporate information with them when leaving a company"

(Dell End User Security Survey 2017, https://datasecurity.dell.com/wpcontent/uploads/2017/09/Dell-End-User-Security-Survey-2017.pdf

LITIGATION TRENDS

In 2017, U.S. trade secret case filings saw an increase up to 1,134 cases filed.

Through the first half of 2018, 581 trade secret cases have been filed, putting this year on pace to slightly exceed the number of trade secret cases in 2017. (Lex Machina Trade Secret Litigation Report 2018)



(Ellmore, Willamette Forensic Analysis Insights, Spring 2016)

CHOICE OF LAW

Texas Law:

- Texas Uniform Trade Secrets Act (TUTSA)
- Texas Harmful Access by Computer (THACA)

Federal Law:

- Defend Trade Secrets Act (DTSA)
- Computer Fraud and Abuse Act (CFAA)

TEXAS UNIFORM TRADE SECRETS ACT

CPRC 134A

(6) "Trade secret" means all forms and types of information, including business, scientific, technical, economic, or engineering information, and any formula, design, prototype, pattern, plan, compilation, program device, program, code, device, method, technique, process, procedure, financial data, or list of actual or potential customers or suppliers, whether tangible or intangible and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if:

(A) the owner of the trade secret has taken reasonable measures under the circumstances to keep the 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, another person who can obtain economic value from the disclosure or use of the information.

(3) "Misappropriation" means:

(A) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or

(B) disclosure or use of a trade secret of another without express or implied consent by a person who:

(i) used improper means to acquire knowledge of the trade secret;

(ii) at the time of disclosure or use, knew or had reason to know that the person's knowledge of the trade secret was:

(a) derived from or through a person who used improper means to acquire the trade secret;

(b) acquired under circumstances giving rise to a duty to maintain the secrecy of or limit the use of the trade secret; or

(c) derived from or through a person who owed a duty to the person seeking relief to maintain the secrecy of or limit the use of the trade secret; or

(iii) before a material change of the position of the person, knew or had reason to know that the trade secret was a trade secret and that knowledge of the trade secret had been acquired by accident or mistake.

TEXAS HARMFUL ACCESS TO COMPUTERS ACT

"A person commits an offense if the person **knowingly accesses a computer, computer network, or computer system without the effective consent of the owner**." Tex. Penal Code § 33.02(a).

"A person who is injured or whose property has been injured as a result of a violation under Chapter 33, Penal Code, has a **civil cause of action if** the conduct constituting the violation was committed **knowingly or intentionally**." CPRC § 143.001(a).

***Miller v. Talley Dunn Gallery, LLC*, 05-15-00444-CV, 2016 WL 836775, at *12 (Tex.App.-Dallas Mar. 3, 2016, no pet. h.)**

FEDERAL DEFEND TRADE SECRETS ACT

"An owner of a trade secret that is misappropriated may bring a civil action ... if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." 18 U.S.C. § 1836(b)(1)

(3) REMEDIES.—In a civil action brought under this subsection with respect to the misappropriation of a trade secret, a court may—

(A) grant an injunction—

(i) to prevent any actual or threatened misappropriation described in paragraph (1) on such terms as the court deems reasonable, provided the order does not—

(I) 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; or

(II) otherwise conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business;

(ii) if determined appropriate by the court, requiring affirmative actions to be taken to protect the trade secret; and

(iii) in exceptional circumstances that render an injunction inequitable, that conditions future use of the trade secret upon payment of a reasonable royalty for no longer than the period of time for which such use could have been prohibited;

(B) award—

(i)

(I) damages for actual loss caused by the misappropriation of the trade secret; and

(II) damages for any unjust enrichment caused by the misappropriation of the trade secret that is not addressed in computing damages for actual loss; or

(ii) in lieu of damages measured by any other methods, the damages caused by the misappropriation measured by imposition of liability for a reasonable royalty for the misappropriator's unauthorized disclosure or use of the trade secret;

Computer Fraud and Abuse Act

(a) Whoever—

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby … (C) obtains information from any protected computer

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value….

18 U.S.C. § 1030(a)(2)-(4)

"Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief…

18 U.S.C. § 1030(g)

LITIGATION TRENDS - RESULTS

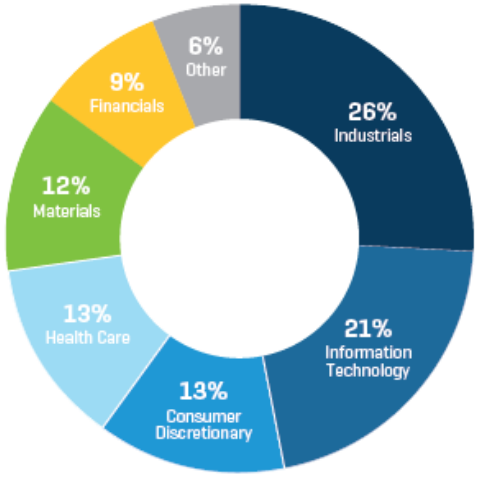
CASE RESOLUTIONS

A striking data point was the proportion of rulings in favor of plaintiffs. Of the cases that ultimately resulted in a verdict, plaintiffs received a favorable ruling 69% of the time, while defendants/counterclaimants received a favorable ruling in only 24% of cases, with split decisions occurring in the other 7%.

Favorable Rulings

69% Plaintiffs / 24% Counterclaimants

FIGURE 4:
Case Activity by Industry Sector



Median damage award nationwide: $2.2 million

"In Texas, the most frequent trier of cases, the average damage award is less than half the size of the overall national average."

Stout Advisory, Trends in Trade Secret Litigation Report 2017

(Review of 248 federal trade secret cases, 1990-2015)

Best Practices For Employers

- Written confidentiality and non-disclosure agreements in place.
- Internal audits to make sure agreement signed by employees, consultants, and key suppliers.
- Employee handbook addressing confidentiality, computer access, and return of company files.
- Mark documents confidential.
- Password protect, and encrypt computers and devices.
- Limit USB and cloud accounts to legitimate business purposes.
- Exit interviews and checklist.
- Severance agreement with claw-back in case of breach.
- Forensic imaging of devices.
- Reminder letter for post-employment obligations.
- Cease and desist letter if trade secret theft is suspected.

Best Practices For Employees

- Don't sign generic NDAs.
- Return physical files.
- New job, new computer.
- Don't carry away design drawings or customer lists.
- Avoid mass downloading or copying of files to USB drive.
- Company files company email.
- Get legal advice when asked to sign a severance agreement.
- Request copies of all agreements from HR.
- Avoid social media posts that attract undue attention.
- Document general knowledge, skill, experience and contacts.
- Know your rights under the Texas Citizens Participation Act (TCPA).

Common Pitfalls With Confidentiality Agreements

- Not having a signed confidentiality agreement.
- Waiting until employment ends to address confidentiality.
- Not having a written agreement with all key personnel (employees, independent contractors, suppliers, vendors).
- Mutual NDA that does not explain what is confidential.
- Agreement that does not require return of company files.

COMPUTER ACCESS POLICIES

- For a CFAA claim "exceeds authorization" is a key battleground. For a THACA claim, "effective consent" is a key battleground.

- Does your company have a written policy restricting:
  - Use of personal email accounts.
  - Forwarding company emails to personal email accounts
  - Downloading files to USB/external hard drive.
  - Cloud-based file sharing sites (Dropbox/Google Docs, etc.)

- What limits does your company place on copying files, keeping files and returning files at or near the end of employment?

Marking Documents Confidential

- Mark key documents "Confidential" (Paper or PDF)

- Virtual data rooms with audit logs (Firmex, ShareFile, Share Vault, etc.)

- Two-factor authentication

Exit Interview

- Who are you going to work for?
- Have you already accepted a job offer?
- What will you be doing?
- Have you returned all company devices?
- Have you returned all company files?
- Are you taking any information with you?

https://www.shrm.org/resourcesandtools/legal-and-compliance/employment-law/pages/when-employees-leave-make-sure-trade-secrets-are-protected.aspx

SEVERANCE AGREEMENTS AND CLAW BACK

- Claw-back provisions create accountability and financial consequences for violating post-employment restrictions.

- Texas Supreme Court has upheld provisions clawing back outstanding unvested stock options for detrimental activities. *See Exxon Mobil Corp. v. Drennan*, 452 S.W.3d 319 (Tex. 2014) ("forfeiture clauses in non-contributory profit-sharing plans, like the detrimental activity provisions … clearly are not covenants not to compete).

- However, some courts have found that taking back pay already awarded as a penalty for quitting is an unlawful restraint of trade. *Rieves v. Buc-ee's Ltd*. 532 S.W.3d 845 (Tex. App.—Houston [14th Dist.] 2017, no pet.).

GENERALLY KNOWN OR GENERALLY STOLEN?

- Trade secret disputes often turn on whether information is "generally known" or whether specific files, lists, or databases were taken.

- Under TUTSA, an employee cannot be enjoined from using "general knowledge, skill, experience."

- "Actual or threatened misappropriation may be enjoined if the order does not prohibit a person from using general knowledge, skill and experience that person acquired during employment."

Tex. Civ. Prac. & Rem. Code 134A.003.

BRAVE NEW WORLD OF TCPA

- The Texas Citizens Participation Act is a departing employee's friend. Tex. Civ. Prac. & Rem. Code 27.001.

- The TCPA can be used as a defense to trade secret claims. *Elite AutoBody v. Autocraft Bodywerks,* 520 S.W.3d 191 (Tex. App.—Austin 2017, pet. dism'd by agr.) ("the Texas Citizens Participation Act (TCPA) … can potentially be invoked successfully to defend against claims seeking to remedy alleged misappropriation or misuse of a business's trade secrets or confidential information.").

DISCLAIMERS

This Presentation is not intended to serve as legal advice.

The facts of each case vary. You should consult a lawyer regarding the specific facts of your case.

This Presentation does not create an attorney-client relationship or form the basis of any contract for legal services.

Conclusion

- Q & A Session

Wesley G. Lotz, Partner

Fulkerson Lotz LLP

4511 Yoakum Blvd., Suite 200

Houston, Texas 77006

713-654-5830

wlotz@fulkersonlotz.com