FOLEY & LARDNER LLP

TEXAS GULF COAST HFMA SUMMER CONFERENCE

Trade Secrets: Best Practices and Enforcement

September 18, 2024

Overview

- Statutory Overview
- Trade Secret Overview
- Avoiding Exfiltration
- Restrictive Covenants
- Take Aways

What Is a Trade Secret

- Information, including a formula, pattern, compilation, program, device, method, technique, or process that:
  - Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, one persons who can obtain economic value from its disclosure or use; and
  - Is the subject of efforts that are reasonable under the circumstances to maintain it secrecy.

This is too complicated-let's just patent the information… right?

Trade Secret or Confidential Information: What's the difference?

- Are the following items: (a) trade secrets or (b) confidential information?
  - LinkedIn contacts
  - Public information compiled together
  - Phone photos / contacts
  - Customer phone numbers and email addresses
  - List of customer names
  - Patented Information

Trade Secret Laws / Protections in the United States

- Federal Defend Trade Secrets Act (DTSA)
- Texas Uniform Trade Secrets Act (TUTSA) – each state has a different version
- Protecting American Intellectual Property Act – January 2023 – criminalizes theft of trade secrets for foreign individuals and companies
- Economic Espionage Act of 1996 - criminalizes theft of trade secrets, does not preempt civil trade secret cases (Definitions broader than DTSA/TUTSA)

- **Confidentiality Agreements**

Defining A Trade Secret – DTSA vs. UTSA

DTSA	Texas (TUTSA)
All forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing	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.
Owner thereof has taken reasonable measures to keep such information secret	The owner of the trade secret has taken reasonable measures under the circumstances to keep the information secret

Defining A Trade Secret

DTSA	Texas (TUTSA)
Acquisition of a trade secret of another by a person who know or has reason to know that the trade secret was acquired by improper means	Identical to DTSA except for formatting
Disclosure or use of a trade secret of another without express or implied consent by a person who – used improper means to acquire knowledge of the trade secret; at the time of disclosure of use, knew or had reason to know that the knowledge of the trade secret was – derived from or through a person who had used improper means to acquire the trade secret; acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret; or derived from or through a person who owed a duty to the person seeking relief to maintain the secrecy of the trade secret or limit the use of the trade secret; or 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 knowledge of the trade secret had been acquired by accident or mistake.	Identical to DTSA except for formatting

Defining A Trade Secret

DTSA	Texas (TUTSA)
Injunction • Cannot prevent employment • Cannot conflict with employee mobility laws	Injunctions • Can prevent employment for a limited period of time • Can restrict access to customers, employees

DAMAGES
• Actual Loss
• Unjust Enrichment
• Reasonable Royalty
• Willful and Malicious Conduct
  ○ 2x damages
  ○ Attorneys' Fees
• Bad Faith Attorneys Fees Claim for Defendants
	DAMAGES
	• Same damages

Seizure Orders	None
Whistleblower/Immunity notice required in Conf. Agreements to obtain attorney's fees	None

Drafting a Confidentiality Agreement for DTSA / enforcement

Notwithstanding the foregoing, Employee will 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. An individual who files a lawsuit for retaliation by an employer for reporting a suspected violation of law may disclose the trade secret to the attorney of the individual and use the trade secret information in the court proceeding, if the individual (x) files any document containing the trade secret under seal; and, (y) does not disclose the trade secret, except pursuant to court order.

Trade Secret Protection: Confidentiality Agreements

- Written Confidentiality Agreements
  - Use in court
  - Demonstrate efforts to protect information
  - Remedies
- Employee Education
  - Onboarding
  - Exit Interview
  - Amnesty
- Notification to Future Employers

Who is Responsible for Trade Secrets?

- Onboarding
- Training
- Exit Interviews

- Contracts
- IP Process
- Training

- Electronic records storage
- Controlling Access
- Monitoring and Auditing Access

- Innovations
- Limited Access Facilities
- Rumor mill (new product launch by competitor after former employee joined them)

- Customer Lists
- Pricing
- Rumor mill (new product launch by competitor after former employee joined them)

- Limited Access Facilities
- Secret Sauce

- Communication
- Training

Protection Lifecycle: Employee Onboarding

- Tip Off– set the rules of the game from the opening tip.
- Handbook with sign-off
  - Confidentiality provision
  - Return-of-property provision including devices, documents, copies, etc.
  - Maintain proof of sign-off
- MVP: Confidentiality Agreement
- Policies
  - No using personal email account
  - No posting information on social media
  - No unauthorized sharing with clients or customers
- Training
  - Teach employees about what can and cannot be shared, and how to share

Protection Lifecycle: Employment

- Employer controls the ball during employment
- Monitor:
  - Have systems in place to spot abnormalities (i.e., email, access, downloads)
  - Social media
- Restrict access:
  - To the building
  - If possible, to the physical information (i.e., scouting reports under lock and key)
  - Or digitally, through password protected shared drives
- Avoid / Prohibit:
  - Flash drives, drop boxes, google drive, etc.
  - Personal email use
  - Personal devices
  - Oversharing with clients and customers or other third parties
- Disclaimers (not just boilerplate)
  - On all protected documents
  - In emails
- TIME OUT: continuing education, risk evaluation

Constant Vigilance!

- Easy to become passive during employment
- Do not make assumptions about “good” and “bad” employees
- Keep policies, training, etc. up to date
- Do not wait until something goes wrong to think about trade secrets

Halftime: You make the Call!

- True or False: Prudent businesses hire full time data watchers to look for anomalies or red flags?
- True or False: We have non-competes, so we don't really need to worry about stuff.
- True or False: Since we are talking about theft, there are criminal penalties as well as civil consequences.
- True or False: We're a great place to work, this would never happen to us!
- True or False: There is really not much we can do except respond.

Employee Lifecycle: Separation

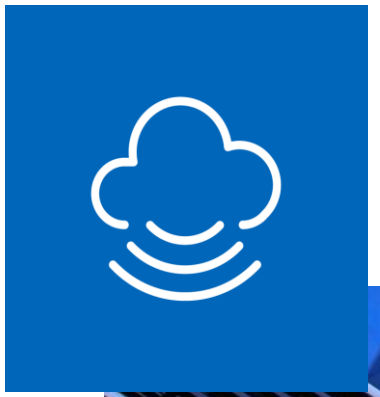
- Stay on Offense
  - Remind / educate employees of obligation
  - Inquire about future plans
- But Remember: Defense is Key
  - Preserve electronics, including accounts and devices
  - Cursory review for any Technical Fouls
    - Emails, downloading, uncommon access
  - Keep in touch with your clients and prospects
- Look for the Flagrant Fouls
  - Opening a competing business
  - Trade in the Honda for a Ferrari

Employee Lifecycle: Enforcement

- Contact counsel and IT Specialist for ESI review
  - Potential Foul: Must properly preserve data!
- Conduct internal investigations – and act FAST
- Is Official Review needed?
  - Reach out to new employer
  - Judicial intervention– Immediate relief

Primary Risk Factors [Exfiltration]

- Employees allowed to use personal cloud/iCloud storage or personal cell phones during employment
  - Dropbox through personal email
- Ability to use external storage devices / USBs
- Ability to access personal email on company computers
- Use of third-party communication services:
  - WhatsApp, WeChat, Snap Chat



Trade Secret Controls

- **Electronic Records**
  - Limited Access
  - Ability to Monitor Access
  - Ability to Audit Access
  - Where are the electronic records?
    - Cloud
      - Where is the “cloud”?
    - Local devices
  - Marking
- **Physical Records & Facilities**
  - Access Controls
    - Locks
    - Badge access
      - Ability to monitor
      - Ability to audit
    - Security cameras
    - Security guards
  - Visitor NDA
  - Marking
- **Employees**
  - Employee NDA
  - Confidential Information Policy
  - Onboarding
  - Training
  - Exit Interviews
- **Third Parties**
  - NDA
  - Commercial Agreements

How Secure is Confidential Information in the Office?

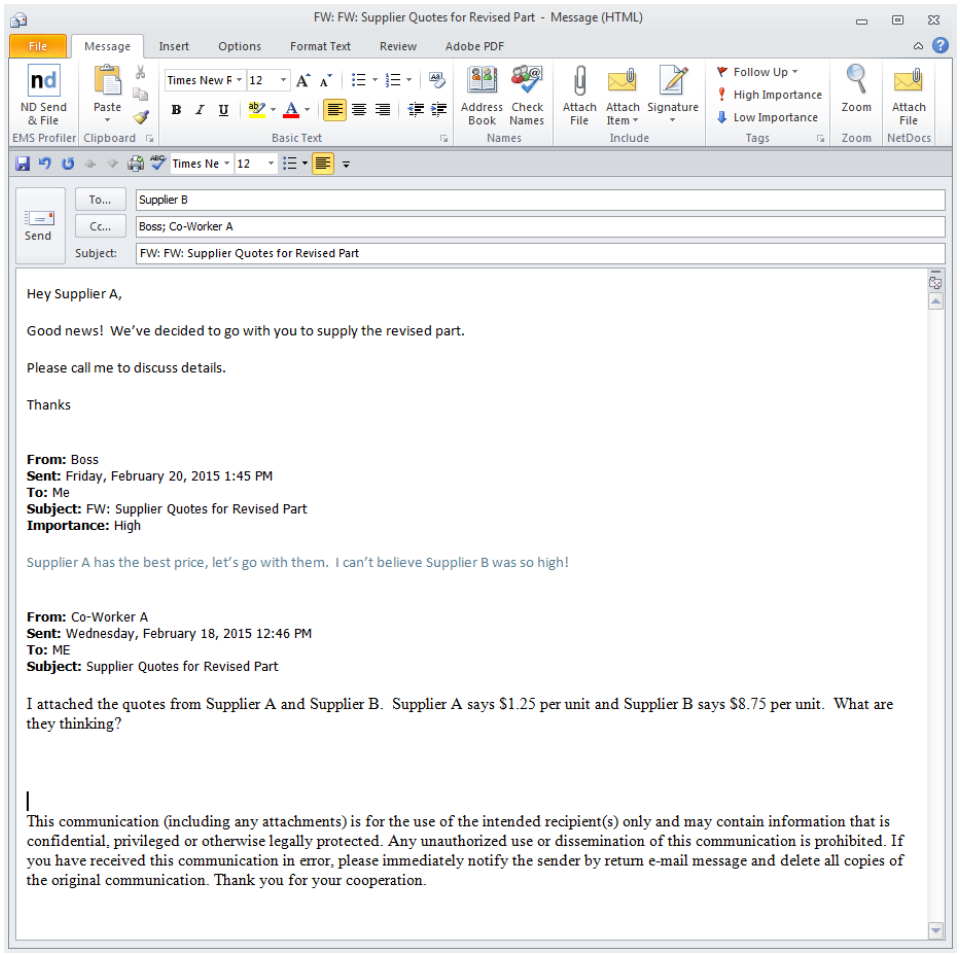
- Who can see your screen?
- What's on your desk?
- Who can hear what you are saying?
- Do you lock out or log off your computer when you leave?
- Do you lock your drawers when you leave?
- Did you leave anything behind when hoteling?

How Secure is Confidential Information at Meetings, Trade Shows, Travel, Public Spaces?

- Are there non-employees in the room/on the call?
  - On site supplier reps?
- Are any notes left on the whiteboard?
- Are any handouts left behind?
- Who can see into meeting room/listen in on call?
- Roll call for conference calls / video conference?
  - Who is that random dial-in on Teams?

How Secure is Confidential Information in Email?

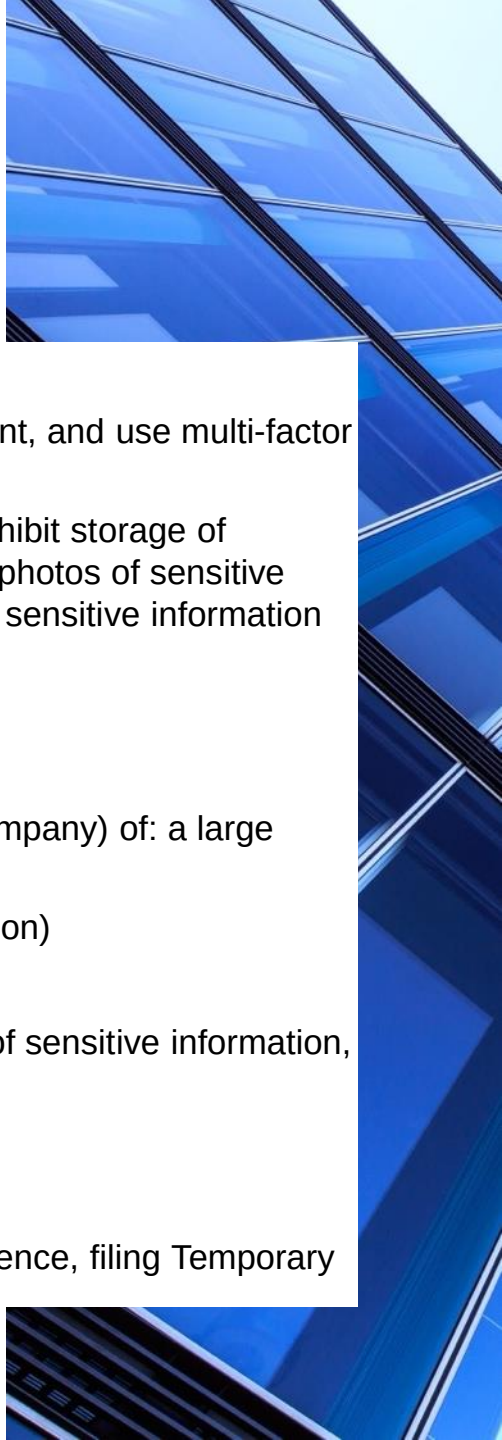
- Who is included in Reply All?
- What information is in the entire e-mail chain?
- Who did you send the e-mail to?
  - Did autocomplete send the e-mail to the wrong “Jeff”?



Real World Example - How Secure is Confidential Information?

- NBA player's agent tweeted a photo of contract signing in front of a white board that appears to list team's targets for possible trades and free agent signings.

Prevent, Detect, and Address Theft of Trade Secrets



- **Actions to Prevent Theft**
  - Access Control: Implement strict access controls to limit the number of employees that have access to sensitive content, and use multi-factor authentication and role-based access to restrict such access
    - Examples: 1) limit read/write/download/transfer/print permissions to networked folders with sensitive content; 2) prohibit storage of sensitive content on non-Company devices and cloud drives, such as dropbox, gdrive and icloud; 3) prohibit taking photos of sensitive products and UIs; 4) encrypt sensitive information at rest and in transit to prevent unauthorized access; 5) separate sensitive information from other less-sensitive data; 6) termination of electronic and physical access upon employee exiting Company
- **Actions to Detect Theft**
  - Monitoring and Auditing: Automatically detect and report abnormal network activity and file access behavior
    - Examples: 1) automatically detect and report the download or transfer (via external drive or e-mail outside of Company) of: a large number of files, a file with a large file size, or files containing certain keywords
  - Establish mechanism for anonymous reporting of suspected theft (e.g., phone line, SMS, online portal, mobile application)
  - Strict exit procedures
    - Examples: 1) exit interview; 2) review access logs documenting historical activity on network, including the access of sensitive information, for abnormal behavior (e.g., increased access prior to exit); 3) identify new employer and start date
- **Actions to Address Theft**
  - Establish a cross-department SWAT team trained to execute a specific plan to address suspected theft
    - Examples: 1) team includes a member from each of IT, Engineering, Legal, and HR; 2) plan includes: securing evidence, filing Temporary Restraining Order, and contacting authorities

What Companies Should Do Now (trade secrets)

- Review/Implement confidentiality policies and agreements
  - This aids the “reasonable measures” argument; TUTSA allows dual claims for breach of confidentiality agreements and trade secret misappropriation
- Establish policies on use of cloud storage, removable USB thumb drives, personal email for work purposes, etc.
- Track metadata – IP policies should restrict access, track the removal of information from Company systems, and allow security access/review.
- Employment policies should outline privacy expectations

National Trend Away From Non-Competes

- FTC proposed non-compete ban.
- Colorado became the first state to impose criminal penalties for seeking to enforce an unenforceable non-compete.
- Many states now set an income threshold to limit the number and types of employees that can be subject to a non-compete.
- In Texas, even where non-competes are not so limited by law, the Courts are not inclined to grant injunctive relief that will put an individual out of work.

Protecting IP if the Rule Survives

- If the Rule survives in whole or part, consider alternative forms of protecting intellectual property:
  1. **Reasonably tailored nondisclosure agreements**
     - "[N]othing in the final rule prevents employers from entering new NDAs with workers"
     - But, NDAs may be impermissible non-competes if "they span such a large scope of information that they function to prevent workers from seeking or accepting other work or starting a business after they leave their job"
     - E.g., NDAs that bar workers from disclosing in their next job any information that is "usable in" or "relates to" the industry in which they work or NDAs disclosing any information or knowledge the worker may obtain during their employment whatsoever, including publicly available information
  2. **Appropriately tailored invention assignment agreements**
     - Agreements that give employers certain rights to inventions created by employees during their employment with a firm
     - Endorsed in the Rule as a less restrictive means of protecting IP

Protecting IP if the Rule Survives

- If the Rule survives in whole or part, consider alternative forms of protecting intellectual property:
  3. **Trade Secret Law**
     - "[T]rade secret law provides employers with a viable, well-established means of protecting investments in trade secrets, without the need to resort to the use of non-competes"
     - 47 states and DC have adopted the Uniform Trade Secrets Act, which provides a civil cause of action for misappropriation of trade secrets
     - So does the federal Defend Trade Secrets Act, which also authorizes in "extraordinary circumstances" civil *ex parte* orders for the seizure of property necessary to prevent dissemination of trade secrets
     - Prepare for likelihood of increased trade secret litigation after employee leaves the company
  4. **Patent Law**
     - "[P]atent law provides companies with a less restrictive alternative than non-competes for protecting [IP]"

Non-Solicitation Provisions Require

- Reasonable limits on:
  - (1) time (≤ 2 years);
  - (2) customer scope; and
  - (3) scope of activity to be restrained.

What Companies Should Do Now (Non-Solicitation)

- Review/Revise non-solicitation agreements
  - Is it two years or less?
  - Is it limited to the customers the employee had business contact with or gained confidential information about during employment?
  - Is it limited to restricting the same type of activity (e.g. sales of widget X) that are similar to what the departing employee sold for the Company?

What Companies Should Do Now (Non-Solicitation)

During Employee's employment with the Company, and for a period of one (1) year thereafter, Employee will not directly or indirectly solicit or conduct business with Company customers or distributors (or prospective customers or distributors) with whom Employee had a business relationship or about whom Employee learned confidential information, during the last two years of Employee's employment, for business, products, goods, or services offered by Company as of the date of Employee's separation from the Company or for business, products, goods, or services that are a substitute for those offered by the Company, or for business, products, goods, or services that as of the date of Employee's separation, the Company was planning to offer to Company clients or prospective clients in the near future.

Thank you

- Any Questions?

Jessica Glatzer Mason
Trade Secret/ Employment Partner

Foley & Lardner LLP
T: 713.276.5793
E: jmason@foley.com

FOLEY
FOLEY & LARDNER LLP

About Foley

Foley & Lardner LLP is a preeminent law firm that stands at the nexus of the energy, health care and life sciences, innovative technology, and manufacturing sectors. We look beyond the law to focus on the constantly evolving demands facing our clients and act as trusted business advisors to deliver creative, practical, and effective solutions. Our 1,100 lawyers across 25 offices worldwide partner on the full range of engagements from corporate counsel to IP work and litigation support, providing our clients with a one-team solution to all their needs. For nearly two centuries, Foley has maintained its commitment to the highest level of innovative legal services and to the stewardship of our people, firm, clients, and the communities we serve.

FOLEY

FOLEY & LARDNER LLP

FOLEY.COM