PORTER|HEDGES

New Year, New Employment: Trade Secret Mishaps and Best Practices

January 18, 2022

Laura Alaniz | 713.226.6647 | lalaniz@porterhedges.com
Derek Forinash | 713.226.6614 | dforinash@porterhedges.com

Agenda

1. Protecting Company Data
2. Confidential Information v. Trade Secret
3. Reasonable Measures for Protecting Confidential Information
4. Best Practices for Protecting Confidential Information
5. Don't Hire A Lawsuit
6. Beware of the Departing Employee
7. Takeaways

Protecting the Company's Data

The Great Resignation

American economy is seeing unprecedented movement in the job market

- November 2021
  - 10.6 million open jobs (6.6%)
  - 6.6 million new hires (4.5%)
  - 4.5 million "quits" (3%)

Movement of Employees

- **Departing employees**
  - Continue to be major vector for loss of confidential information and trade secrets ("trade secret assets")
  - Additional challenges from remote working (exit procedures, accounting for company property, etc.)

- **New employees**
  - Source of third party information coming into your company – creating substantial liability
  - Lack of familiarity with company security and IT protections

So what do I do?

- Most executives realize their company's confidential information is critical and essential to business
- In many businesses, trade secrets are most important intellectual property asset, greatly exceeding value of patents, trademarks, and other "hard" IP assets
- Despite this understanding, confidential information is usually not well managed or sufficiently protected

Confidential Information v. Trade Secret

What is Confidential Information?

Information or data that is not generally known or accessible and which gives the owner a competitive advantage.

Examples include the following:

- Technical information
- Know-how
- Technology
- Equipment Specs
- Trade Secrets
- Intellectual Property
- Plans or Drawings
- Formulas
- Agreements
- Financials
- Sales or Marketing Strategy
- Research Data
- Profit & Loss Data
- Business Plan
- Procedures
- Customer Lists
- Customer Profiles
- Pricing/Proposals

What is a Trade Secret?

- The information is not known or available to the public and is used by the company directly for business
- The information provides the company with an economic advantage
- The company takes reasonable efforts to protect the secrecy of the information

Example include:

- Formulas
- Manufacturing methods
- Food/drink recipes
- Customer lists
- Business plans
- Industry forecasts
- Marketing plans
- Research and development data
- Pricing and profit margin information
- Business manuals
- Computer programs, scripts, algorithms

Overview of Federal Trade Secrets Law

U.S. Defend Trade Secrets Act (DTSA)(2016) broadly defines trade secrets to include all forms and types of information IF:

- Owner has taken reasonable measures to keep information secret; and
- Information derives independent economic value from not being generally known to, and not being readily ascertainable by, another person who can obtain economic value from disclosure or use
- **Does not prevent** reverse engineering

Overview of Texas Trade Secrets Law

Texas followed common law until passage of Texas Uniform Trade Secrets Act (TUTSA) in 2013

- Trade secrets are information that:
  - Include formula, pattern compilation, program, device, technique, process, financial data, or list of actual or potential customers or suppliers;
  - Derives independent economic value from not being generally known to, and not being readily ascertainable by, another person who can obtain economic value from disclosure or use; and
  - Subject of efforts reasonable under the circumstances to maintain its secrecy
- **Does not prevent** reverse engineering

Beware

Information can lose its status as confidential information or a trade secret if it is:

- Generally known at time of disclosure
- Rightfully received from a third party authorized to make disclosure
- Publicly known through no fault of the recipient

Unintentional disclosures count

- Presentations at conferences/trade shows
- Sales activities, product demos, bid proposals without confidentiality agreements
- Investor/ analyst presentations
- Poor Document Control
  - Documents visible in public places
  - Information left behind in conference rooms, etc.

Bottom-line

Confidential information that goes outside of the organization without an obligation of confidentiality – even if disclosed to only one person – is no longer confidential.

Reasonable Measures for Protecting Confidential Information

Confidential Information Management

Stages of CI Asset Management

- Must be done in order

- Identification
- Classification
- Protection

Confidential Information Asset Management

- Identification – What are the company's CI assets?
- Classification – How important are each of those assets, practicality of asset being kept secret?
- Protection – What reasonable measures can be taken to protect the asset?

Identification and Classification

Identification

- What is the information?
- Where is it kept?
- Who is the controller of the information?

Classification

- Who needs to know it?
- How hard is it to keep secret?
- What did it cost to develop?
- What would the value be to a competitor?

Protection

- Publicize the existence of confidential information without publicizing the information
- Robust confidentiality provisions in contracts, employee handbooks, bid offers, and other business documents
- Physical and IT protection
  - Secure servers
  - Password protection
  - ID cards, visitor escorts
  - Data transmission restriction/monitoring

Best Practices for Protecting Confidential Information

Hiring and Onboarding: Key Agreements

- Invention assignment agreements
- Non-disclosure and trade secret protection agreements
- Non-solicitation and Non-competition clauses in agreements

Hiring and Onboarding: Key Agreements and Policies

- Social media policy and social media ownership agreements
- Computer use and access policies
- Employee handbook provisions regarding monitoring and code of conduct

Hiring and Onboarding: Key Procedures

- Conduct new hire training on the importance of protecting your company's assets
- Separate out trade secret agreements and training from the piles of paperwork and training that new employees receive
- Periodically follow up with all employees to ensure continued compliance with policies and agreements put in place to protect confidential information

Off-Boarding: Exit Interviews

- Make sure you have an exit interview
- Check employee's computer activities and work activities in advance of the meeting
- Ask questions about employee's new job and about the information to which employee had access
- If there are any concerns about suspicious activities related to company property and computer access/ usage, ask the employee about those activities

Off-Boarding: Exit Interviews

- Assess the credibility of the employee during the interview
- Consider using an exit interview certification in which the departing employee acknowledges or certifies his or her understanding of his or her continuing confidentiality obligations
- Ensure that all company property, hardware, and devices have been returned
- Follow-up with business team regarding the exit interview and any special handling

What to do about Remote Working?

Identify High Value, High Risk Areas

Prioritize your security measures by broadly identifying the high value and high risk areas of your business, where the confidential information and trade secrets are most important to protect or are most vulnerable during the pandemic, including:

- High value/risk business divisions, departments or teams,
- High value/risk products or services, and
- High value/risk servers, networks, drives, computers or other media

Address the Risks Associated with Remote Work

- Remind your employees that working remotely does not create any exception to existing confidentiality and non-disclosure agreements or company policies, manuals, or practices

- Establish and distribute a clear telework policy

- Employers should consider requiring teleworking employees to sign (or e-sign) the policy before granting them remote access to confidential information

Limit and Track Your Third-Party Disclosures

When sharing confidential information or trade secrets with third parties, make sure you document the following key information:

- What information was shared?
- When?
- With whom?
- For what purpose?
- Under what agreements and restrictions?
- Was the information returned or destroyed as required after the project was complete?

Limit and Track Your Third Party Disclosures

- Maintaining this information is important for the following reasons:
  - Ensures that third parties protect your information
  - Be used as proof in any later dispute over the unauthorized use of your information
  - Helps minimize the risk of successful claims by third parties over the alleged unauthorized use of their information

- Train employee that securing critical trade secrets and confidential information remains a high priority even if company gets urgent or unexpected requests, demands or opportunities

Adapt Your Off-Boarding Procedures

Many off-boarding procedures can be performed remotely, including:

- Disabling access to company systems, electronic devices (cell phone or tablets), and accounts, and monitoring any unauthorized access thereafter
- Conducting an exit interview by video or phone
- Requiring e-signature of documents establishing the off-boarded employee's continuing confidentiality obligations

Adapt Your Off-Boarding Procedures

How to handle return of company property and information?

- Take inventory of all company property and information the employee has taken off site
- Confirm this inventory with the employee during the exit interview
- Send packing materials with a prepaid label for employee to return company property and documents
- Establish a plan for the secure destruction and/or return of this property and information if employee is not cooperative

Don’t Hire A Lawsuit

How to Protect Your Company

- Put in place agreements and policies relating to former employers' trade secrets
  - Advise the new employee in writing that your offer of employment is not based on his or her knowledge or possession of any previous employer's confidential information
  - Consider having the new employee sign an acknowledgement (free standing or in a non-disclosure agreement) affirming that not use former employers' information
  - Periodically review the new employee's work to confirm that he or she is not utilizing confidential and proprietary information belonging to previous employers

Beware of the Departing Employee

Warning Signs of Trade Secret Theft

Suspicious Employee Conduct

- ⚠ Exposure to sensitive information and departure
  - ⚠ Sudden,
  - ⚠ Surprising
  - ⚠ Suspicious
- ⚠ Refusing to account for company assets on exit
- ⚠ Suspicious or frequent use of external drives
- ⚠ Unapproved use of VPN or cloud services
- ⚠ Forwarding to personal email or other external addresses
- ⚠ Access large amounts of documents before departure
- ⚠ Data loss prevention alerts

Warning Signs of Trade Secret Theft

Suspicious Departures

- ⚠ Multiple resignations within a group
- ⚠ Employee leaving to work for competitor
- ⚠ Employee leaving to work with other ex-employees
- ⚠ Employee not willing to divulge new employer on exit
- ⚠ Employee leaving for start-up company in the same field
- ⚠ Disgruntled employee
- ⚠ Employee part of RIF or furlough

Warning Signs of Trade Secret Theft

Competitive Conduct

- ⚠ New company with former employee(s) launches competitive business
- ⚠ New company with former employee(s) announces competing product very quickly
- ⚠ Suspicious customer contacts
- ⚠ Suspicious vendor contacts
- ⚠ Tips

Steps to Protect Your Company from Departing Employee

- Interview co-workers to gather additional information regarding the departing employee's intentions and any suspicious activities

- Disable the departing employee's access to the facility and company computers

- Inspect the employee's office and review hard copy files to ensure that company materials have not been compromised, taken, destroyed or altered

Steps to Protect Your Company from Departing Employee

- Review the employee's recent e-mail, computer system activity, and voicemail

- Review the employee's expense reports and cell phone records to determine if he or she is preparing to exit with any customers

- Follow up with customers that the departing employee was servicing

Steps to Protect Your Company from Departing Employee

- Consider sending a letter to the new employer informing them of the employee's obligations to the company, as well as the employee

- Sequester the employee's computer and other electronic devices for forensic analysis
  - Use a professional
  - Preserve the employee's emails

Identify, Collect, and Preserve Evidence

- Examples of useful evidence:
  - Employee hard drives
  - Employee mobile devices
  - Enterprise email archives
  - Document record system history
  - Server data
  - USB history
  - Internet history
  - Cloud storage usage/uploads
  - Calendar appointments/contacts
  - Chat history
  - DLP records

- Stop any automatic or process driven deletions and computer reassignment

Takeaways

Takeaways

- Have written policies, agreements, and procedures in place to protect your company data
- Be deliberate in on-boarding due diligence
- Conduct thorough off-boarding
- Identify any special procedures that need to be implemented due remote work
- Take necessary actions if you suspect that your company data has been misappropriated

Thank you.

Questions?

Laura Alaniz

Laura Alaniz
Partner
lalaniz@porterhedges.com
713.226.6647

J.D., Baylor University School of Law

B.S., The University of Texas at Austin, high honors

Full Online Biography

Laura Alaniz counsels clients on compliance issues relating to employment law and prevention of claims including issues related to hiring and terminating employees, leaves of absence, layoffs, unemployment compensation, employment handbooks and policies, and conducting employee and management training.

She is also an experienced litigator and advisor focusing on representation of management in all aspects of labor and employment law matters. As a litigator, Laura utilizes her experience to provide guidance to her clients on how to avoid litigation and minimize their risk of claims.

Laura is Board Certified in Labor and Employment by the Texas Board of Legal Specialization and was recognized as one of the "Top 50 Women Lawyers" in Houston by the Texas Diversity Council.

Derek V. Forinash

Derek V. Forinash
Partner
dforinash@porterhedges.com
713.226.6714

J.D., University of Houston Law Center

B.S., Louisiana State University, Mechanical Engineering

Full Online Biography

Derek Forinash serves as outside general counsel to private companies and also provides comprehensive IP legal services to a range of clients. His experience includes more than eighteen years in both private practice and as in-house counsel, including serving as Senior Corporate Counsel for an oilfield services company and as Vice President and General Counsel of a Houston-based reservoir engineering company.

As outside general counsel, he provides practical legal advice to private companies on day-to-day issues that impact their business including employment matters, commercial contracts, intellectual property, governance, financial transactions and risk management.

His intellectual property practice focuses on developing, protecting, and monetizing intellectual property portfolios as well as drafting and negotiating technology-related transactions including SaaS agreements, technology licenses, and joint development agreements.

He has represented clients in a wide range of technologies and industries including upstream oilfield technology, petrochemicals, offshore equipment and computer software and hardware. Prior to law school, Derek worked as an engineer designing oilfield equipment.