FTI CONSULTING | TECHNOLOGY

WOMBLE BOND DICKINSON

Practical Tips for Protecting and Enforcing Trade Secrets

Patrick Buckler and James Scarazzo

October 30, 2018

ACC Association of Corporate Counsel
BALTIMORE

“A Survey of In-House Attorney Views On Trade Secrets” - 75% of respondents indicated that risks to trade secrets have increased over the past 10 years and 70% said their company experienced attempted or actual misappropriation of trade secrets

Topics

- What is a trade secret?
- Identify and Take Inventory of Your Potential Trade Secrets
- Conduct an Initial Trade Secrets Audit
- Common Culprits of Trade Secret Theft or Disclosure
- Develop a Trade Secret Protection Plan
- Highlights of Defend Trade Secrets Act

Defend Trade Secrets Act's definition of a trade secret:

1. "all forms and types of financial, business, scientific, technical, economic, or engineering information, . . . whether tangible or intangible"
2. so long as "the owner thereof has taken reasonable measures to keep such information secret" and
3. "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."

Maryland Uniform Trade Secrets Act's definition of a trade secret:

1. "information, including a . . . compilation . . . that"
   a. "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; and"
   b. "is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."

A trade secret is anything that has economic value because it is kept secret.

Identifying and Taking Inventory of Your Potential Trade Secrets

Answer the following:

1. What gives your business a competitive advantage over others in the marketplace?
2. Is there information about your business that your company does not share and would not want anyone outside the company to know because the information could help competitors and/or hurt the company?

Identifying and Taking Inventory of Your Potential Trade Secrets (cont)

Trade secrets may include: (a) Business know-how and processes; (b) Formulas or algorithms; (c) Customer information; (d) Financial information; (e) Business and marketing plans; (f) Product/service pricing

For each potential trade secret, ask the following questions:

1. Is the information secret?
2. Is the information valuable?
3. Is the information known in the industry?
4. Is the information obvious to others?

Conduct an Initial Trade Secrets Audit

- You should have a point person or team spearhead the effort.
- The person or team should do/determine the following:

1. Meet with the department heads within the company to determine what valuable information each department might have.
2. Determine what measures are in place to secure trade secrets:
    a. Location?
    b. Access?
    c. Written policies?
    d. Agreements?

Conduct an Initial Trade Secrets Audit (cont)

e. IT measures?
   - Examine competing requirements
   - Ops / Security / Financial
   - Only provide access necessary to do work
   - User business accounts rather than personal accounts
   - Guard social media
3. Are these measures effective?
4. What additional measures are necessary?
5. How should company discard or identify trade secrets going forward?

Common Culprits of Trade Secret Theft or Disclosure

"A Survey of In-House Attorney Views On Trade Secrets"

1. Former employee – 90% of respondents
2. Competitor – 50%
3. Current employee – 45%
4. Business partner – 30%
5. Customer/client – 15%

Develop a Trade Secret Protection Plan

1. Written trade secret protection plan
2. Segregate and label trade secrets
3. Implement appropriate IT measures
    a. Consider using “Accessed Based Enumeration” – Out of sight – Out of mind
    b. Consider using Data Loss Protection systems
    c. Consider the risks of implementing BYOD (Bring Your Own Device)
    d. Consider using a Mobile Device Management (MDM) system
    e. Consider physical or logical separation of data (store the most sensitive data on a separate server or firewall access to the information)

Develop a Trade Secret Protection Plan (cont)

f. Institute a monitoring program / Log who accessed information.

4. Employee manual should reference the company's trade secret protection plan
5. Employee Orientation and Education
   a. Mandate that new employees not disclose the trade secrets of former employers
   b. Explain that company trade secrets and confidential information cannot be disclosed and that disclosure is grounds for termination
   c. Have appropriate employees sign NDAs
   d. Remind employees at their reviews of the trade secret protection plan and duties under NDAs

Develop a Trade Secret Protection Plan (cont)

6. Types Agreements for Employees
   a. Acknowledgement that employee will not use prior employer's trade secrets and has returned prior employer's property
   b. NDA
   c. Non-compete
   d. Invention assignment agreement – certain states have statutes that govern the scope of such agreements
   e. Computer use and access and BYOD agreements
      - Published acceptable use of computer and equipment policy
      - Use a log on warning and confirmation
      - Use a written BYOD Policy
   g. Social media ownership

Develop a Trade Secret Protection Plan (cont)

7. Customize agreements based on the following:
   a. To what trade secrets does employee have access?
   b. What risks does employee pose with respect to trade secrets?
   c. What would be impact of employee's theft of trade secrets?
   d. What steps need to be taken to secure employee/trade secrets?

Develop a Trade Secret Protection Plan (cont)

8. Agreements for Consultants
   a. NDAs
   b. Work-for-hire
9. Agreements with Others (Business Partners / Customers / Clients / Vendors)
   a. NDAs

Develop a Trade Secret Protection Plan (cont)

10. Exit Process for Employees
    a. Identify the trade secrets the employee accessed
    b. Check employee's computer activities and work activities
    c. Question the departing employee in detail
        - Ask employee why s/he is leaving
        - Ask employee what new position will be
    d. Inform the employee of her/his continuing obligations under any agreements
    e. Consider letter to new employer and employee with reminder of continuing obligations

Develop a Trade Secret Protection Plan (cont)

f. Ensure that all company property, hardware, and devices have been returned, including e-mail and cloud data, and social media accounts
g. Remove all company data from any personal devices
h. Disable access to company networks
i. Obtain user names and passwords for all company social media accounts
j. Consider having departing employee's emails preserved and electronic devices forensically imaged

Develop a Trade Secret Protection Plan (cont)

11. Post-Termination Investigation
    a. Interview employee's co-workers; gauge whether employees are hearing about employee in the marketplace
    b. Examine email activity
    c. Examine phone records
    d. Examine access logs (including email tracking log)
    e. Forensic investigation of employee's computer activities
        - USB connection history
        - Internet searches and activity
        - File server access
        - Get list of all connected mobile devices to email server
        - Disable access to network

Highlights of Defend Trade Secrets Act – enacted in May 2016

"An owner of a trade secret that is misappropriated may bring a civil action under this subsection if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce."

"[A]pplies 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.

Highlights of Defend Trade Secrets Act – enacted in May 2016 (cont)

The claim arises when the misappropriation is or should have been discovered.

Three-year statute of limitations

Elements of a DTSA misappropriation claim are similar to the elements of state law trade secret claims

Highlights of Defend Trade Secrets Act – enacted in May 2016 (cont)

An ex parte seizure order may be obtained only as "necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action."

(1) Immediate and irreparable injury if seizure is not ordered

(2) Harm to the applicant from denying relief must outweigh the harm to the legitimate interests of the person who would be subject to the seizure order

(3) Applicant must be likely to succeed on the merits

(4) Person against whom seizure is ordered must have actual possession of the trade secret

(5) Application must describe with reasonable particularity the matter to be seized and where it is located

(6) Applicant must show that the person against whom the seizure is requested would "destroy, move, hide, or otherwise make such matter inaccessible to the court" if they were given notice.

(7) Applicant must not have publicized the requested seizure

Whistleblower Protection

DTSA includes a whistleblower clause that provides immunity for disclosure of trade secrets to government officials for the sole purpose of reporting violations of the law.

Employers must give notice of that immunity “in any contract or agreement with an employee that governs the use of a trade secret or other confidential information.”

Employers who do not do so cannot recover punitive damages or attorneys’ fees that may otherwise be available under the Act.

Remedies

Plaintiff is entitled to recover actual loss and any unjust enrichment caused by misappropriation that is not adequately compensated by actual loss. Alternatively, plaintiff may recover a reasonable royalty for the unauthorized disclosure or use of the trade secret.

DTSA also provides for exemplary damages of not more than double the compensatory award in the case of willful or malicious misappropriation. Reasonable attorneys' fees may also be recovered in the case of willful or malicious misappropriation.

DTSA specifically provides for injunctive relief to prevent actual or threatened misappropriation.

Patrick Buckler
Of Counsel
Womble Bond Dickinson (US) LLP
e: Patrick.Buckler@wbd-us.com

James Scarazzo
Managing Director
FTI Consulting Technology
e: Jim.Scarazzo@fticonsulting.com