

Protecting Trade Secrets Under U.S. Law

Daniel J. Melman

Phone: (646) 878-0845

DMelman@PearlCohen.com

https://www.linkedin.com/in/daniel-melman-467405a/

OCTOBER 27, 2021

© 2021, Daniel Melman, Pearl Cohen Zedek Latzer Baratz LLP. This presentation and its content are not to be construed as legal advice.

PEARL COHEN



Daniel J. Melman

Partner
Patent and Complex
Litigation

Daniel is a Partner in the Patent and Complex Litigation Group at Pearl Cohen's New York office. He is an experienced intellectual property litigation and trial attorney with a focus on patents, trade secrets, and other complex matters across various technologies and industries. He concentrates his practice on the protection and enforcement of intellectual property assets and defending clients against claims of infringement.

Daniel can be reached at:

DMelman@PearlCohen.com

https://www.linkedin.com/in/daniel-melman-467405a/

Why Focus on Trade Secrets?

- Trade secrets are often an employer's most valuable assets
- Trade secrets can protect key assets that are not protectable under other IP regimes (or not reliably protectable)
- Increasing cross-border misappropriation
- Misappropriation of trade secrets by former employees may have devastating effects
 - Once disclosed, trade secrets may be lost forever
 - Lost competitive edge
 - Lost business and reputational harm



Elements of a Trade Secret

- Must be secret:
 - Not generally known to others
 - Not readily ascertainable
- Independent economic value
 - Secrecy provides an economic advantage over competitors
- Must take reasonable measures to maintain secrecy

Types of Trade Secrets

May include:

- Know-how "secret sauce"
- Technical drawings
- Specifications
- Computer algorithms
- Sales methods
- Marketing strategies

- Distribution methods
- Consumer profiles
- Advertising strategies
- Supplier and client lists
- Manufacturing processes
- "Negative know-how"

What Constitutes a Trade Secret?

• Factors to consider:

- Extent to which the information is known outside of the business
- Extent to which the information is known by employees or others in the business
- Measures taken to guard secrecy of the information
- Effort and money expended to develop the information
- Ease or difficulty with which the information could be lawfully acquired
- Value of the information to the owner and to competitors

Defend Trade Secrets Act ("DTSA")

- New Federal law (2016)
- Federal Court jurisdiction
- Provides for civil and criminal penalties
- Extraterritorial reach (conduct occurring outside the U.S.):
 - U.S. corporations or citizens can be held liable regardless of whether the misappropriation occurred abroad; and
 - An entity can be held liable for foreign misappropriation if "an act in furtherance of the offense was committed in the United States"
 - E.g. Sending emails to recipients in the U.S.; attending U.S. trade shows; recruiting U.S. employees; meeting with vendors in the U.S.

When Are Trade Secrets at Greatest Risk?

- Departing/former employees
- Business partners (e.g., joint ventures/research; vendors; customers)
- Corporate espionage
 - Reverse engineering and independent derivation are generally not prohibited under trade secret law
- Remote work force considerations

Internal Policies and Procedures

- Trade secrets owners must take "reasonable measures" to protect their trade secrets; update practices as technology improves
- Physical/electronic/digital safeguards
- Employment practices
- Response practices
- Confidentiality programs and records management
- Monitoring and auditing
- Disclosure procedures
- Identify the trade secrets of OTHERS clarify obligations and risks



Employment Procedures

- Assess risks during hiring and onboarding
- Require all employees to sign confidentiality agreements
 - Specify obligations at commencement of, during, and after employment
- Education and training; special considerations for remote workforce
- Monitor compliance
- Exit interviews and related procedures
 - Return/seizure of all company property
 - Discontinue access to confidential information via online portals
- Response procedures when theft or misappropriation is suspected



Disclosure Procedures

- ANY disclosure of proprietary confidential information must be protected by written agreements
 - NDA; best and consistent practices (update when necessary)
 - Consider what information to disclose
 - Effective Terms of Use
- Clearly define the confidential information
- Clearly define the purpose of the disclosure
- Clearly define scope of permissible use and disclosure of the confidential information

- Prompt and thorough investigation and action
 - Identify misappropriated information; why is the information taken a secret?
 - Conduct forensic analysis
 - Gather Information about the ex-employee's new employee
 - Gather and document all relevant facts; how did the company act to protect the information?
- Cease and desist letters
 - Remind former employee of contractual obligations (nondisclosure; non-compete; non-solicitation)
 - Demand return of information
 - Consider copying the new employer
 - Consider contacting law enforcement



- Engage outside counsel
- Engage experts in relevant industry; damages experts
- Consider jurisdictional options (contractual choice of law provisions)
- A DTSA action must be brought no later than 3 years after date misappropriation:
 - Was discovered
 - Should have been discovered with reasonable diligence
- Decide whether to include the employee's new employer in litigation
 - Was the employee acting under new employer's direction?
 - Did the new employer gain an unfair competitive advantage?
 - Has the new employer agreed to indemnify the employee?
 - Tortious interference with contract claims



- Inevitable Disclosure Doctrine
 - Absence of evidence of the employee's actual or intended misappropriation, use, or disclosure of trade secrets
 - But, it is impossible for the former employee to perform the new job without relying or using trade secrets
 - "Inevitable" that the former employee will use or disclose the trade secrets and cause harm
 - Competitor companies in niche market
 - Former employee high level executive privy to strategic plans/information

- Injunctive relief
 - Temporary restraining orders
 - Preliminary injunctions; enforce employee restrictive covenants during litigation
 - Evidentiary showing or irreparable harm
 - e.g. loss of customers, loss of goodwill, price erosion; often presumed in TS cases
 - Likelihood that the employer will ultimately prevail
 - Requires quick action and marshalling of supporting evidence
 - Often dispositive of the case
- Expedited discovery
 - Broad and liberal scope
 - litigation holds and document preservation obligations
 - Forensic investigations



- Monetary damages
 - Lost profits
 - Lost market share
 - Wrongdoer's unjust enrichment
 - Reasonable royalty
 - Punitive damages for willful misappropriation
 - Attorneys' fees in exceptional cases



How to Defend a Trade Secrets Case

- The information is not a trade secret
 - Typically, first line of defense
 - Plaintiffs should not overreach on what is claimed as a TS
 - E.g., pricing vs. pricing methodology; customer names vs. customer preferences and discounts; common industry knowledge
- Failure to take reasonable measures to protect
 - Be prepared to explain in detail efforts taken to protect your trade secrets
- Plaintiff's success depends on proactive measures taken before misappropriation occurs



Thank You!

For questions and more information, please contact Daniel J. Melman at:

Phone: (646) 878-0845

Email: DMelman@PearlCohen.com

https://www.linkedin.com/in/daniel-melman-467405a/