Strategies for Litigation Success: Trade Secret Asset Management

The Defend Trade Secrets Act of 2016

Presented by:
R. Mark Halligan, Esq. Partner, FisherBroyles, LLP
rmarkhalligan@fishebroyles.com
21st Century: The Emergence of Trade Secret Assets

- The Defend Trade Secrets Act of 2016
- The European Union Trade Secret Directive
- The ITC: *TianRui Group Co. v. ITC*, 661 F.3d 1322, 1337 (Fed. Cir. 2011)
- The Trans-Pacific Partnership (TPP)
Patents vs. Trade Secrets: The New Calculus

• The United States Supreme Court

• The America Invents Act (AIA): IPR Proceedings

• Costs: Patent vs. Trade Secret Calculus

• International Enforcement Issues
The Defend Trade Secrets Act of 2016

• The DTSA is the pinnacle of years of practice in Trade Secrets Law

• 22 years on John Marshall Law School, Adjunct Faculty, John Marshall Law School.

• 8 Years (and Earlier) Advocating a Private EEA Cause of Action.


A Short Primer on the Historical Background of US Trade Secret Law

› Vickery v. Welch (1837)
› Peabody v. Norfolk (1868)
› Restatement of the Law of Torts: Section 757
  – 6-Factor Litmus Test for Trade Secrets
› The Uniform Trade Secrets Act (1979-1985)
› U.S. Supreme Court Decisions:
  – Aronson v. Quick Point Pencil (1979)
› Restatement (Third) of Unfair Competition (1995)
› Economic Espionage Act of 1996
The Passage of the DTSA

• A watershed event in intellectual property law
  – The Senate passed the DTSA on April 11, 2016 (87-0).
  – The House of Representatives passed the DTSA on April 27, 2016 (410-2).
  – President Obama signed the bill into law on May 11, 2016.
• Trade Secret Assets are no longer stepchild intellectual property rights.
• Trade Secrets are now on the same playing field as patents, copyrights and trademarks.
• There is no preemption.
• Powerful trade secret protection tools—ex parte seizure provisions.
• Fair and Balanced Protections for Defendants.
Two Critical Amendments to the Economic Espionage Act of 1996

• **18 USC Section 1836(b)(1) “Private Civil Actions”**

  “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.”

• **18 USC Section 1836(b)(2) “Civil Seizure”**

  “Based on an affidavit or verified complaint…the court may, upon ex parte application, but only in extraordinary circumstances….”
• “The amendments made to this section [Section 1836] shall apply with respect to any misappropriation of a trade secret [as defined in Section 1839] for which any act occurs on or after the date of the enactment of this Act.”

• No preemption: “The district courts of the United States shall have original [not exclusive] jurisdiction of civil actions brought under this section [Section 1836].

• This chapter [Protection of Trade Secrets] shall not be construed to preempt or displace any other remedies, whether civil or criminal. [Section 1838]
DTSA: Six Phases *Ex Parte Seizure* Process

- (1) Ex Parte Application
- (2) Civil Seizure Order Elements
- (3) Execution of the Civil Seizure Order
- (4) Safeguarding the Seized Trade Secret Materials
- (5) Post-Seizure Hearing
- (6) Proceedings for an Unwarranted or Excessive Seizure Order
“DTSA: “Extraordinary Circumstances”

• “[O]nly in extraordinary circumstances” under Section 1836(b)(2)(A)(i)
  › Objective “to prevent the propagation or dissemination of the trade secret” or “to preserve evidence” based on Section 1836(b)(2)(A)(i) and DTSA House and Senate Reports

• Legislative history examples
  › [1] “a defendant is seeking to flee the country or [2] planning to disclose the trade secret to a third party immediately or [3] is otherwise not amenable to the enforcement of the court’s orders.”
EEA/DTSA:
Trade Secrets and Whistleblowers

• Protect Whistleblowers
• Protect Trade Secrets
• What Activities Receive “Immunity”? 
  › Disclosure of a trade secret to a government official or an attorney solely for the purpose of reporting or investigating a suspected legal violation.
  › Disclosure of a trade secret in a document that is filed under seal in a lawsuit or other proceedings. [anti-retaliation lawsuits].
  › Whistleblower status is not a “license to steal.”
The DTSA “Notice” Provision


• An employer shall provide notice of the immunity set forth in this subsection in any contract or agreement with an “employee” that governs the use of a trade secret or other confidential information.

• For purposes of this section, the term “employee” includes any individual performing work as a contractor or a consultant for an employer.

• Cross-reference to a policy document permitted.

• Non-compliance: No exemplary damages or attorney fees.
The DTSA is built upon the UTSA and EEA

- The Uniform Trade Secrets Act (UTSA) was drafted by the National Conference of Commissioners on Uniform State Laws and approved by the American Bar Association at its meeting in Chicago, Illinois February 4-5, 1980. (1985 Amendments August 2-9, 1985).

- Every State except New York and Massachusetts enacted the UTSA.

- In turn, the UTSA was built upon almost 150 years of common law development of trade secrets: *Vickery v. Welch*, 33 Mass. 523 (1837).
UTSA Substantive Provisions

• Definitions:
  › “Improper Means”
  › “Misappropriation”
  › “Person”
  › “Trade Secret”

• Injunctive Relief: (Actual or Threatened Misappropriation)

• Damages

• Attorney’s Fees

• Preservation of Secrecy

• Statute of Limitations
EEA: The Economic Espionage Act of 1996

• Section 1831: Economic Espionage (foreign government, foreign instrumentality, foreign agent)
• Section 1832: Theft of Trade Secrets
• Extraterritorial Jurisdiction
• Definitions:
  • “foreign instrumentality” and “foreign agent”
  • Upgraded definition of “trade secret” for the Information Age
  • Definition of “owner” of trade secret: “the person or entity in whom or in which rightful legal or equitable title, or license in, the trade secret is reposed.

• No private civil cause of action
Trade Secrets Clarification Act of 2012

• Fixed the defect the interstate commerce requirement that came to light in the reversal of the Aleynikov conviction by the Second Circuit Court of Appeals: *United States v. Aleynikov*, 676 F.3d 71, 75 (2d Cir. 2012)

• 18 U.S.C. Section 1832 (as amended):

• (a) Whoever, with intent to convert a trade secret, that is related to [delete: or included in a product that is produced for or placed in] a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will injure any owner of that trade secret…
EEA/DTSA: Extraterritorial Jurisdiction

• The Economic Espionage Act of 1996 (and now the Defend Trade Secrets Act of 2016) expressly applies to extraterritorial conduct occurring outside the United States. 18 U.S.C. Section 1837.

• The DTSA also amends 18 U.S.C. Section 1835 to include Section 1831 (Economic Espionage) and Section 1832 (Theft of Trade Secrets) as RICO predicate acts in Section 1961(1).

• This now opens the door for civil RICO causes of action based upon conspiracies and attempts to steal trade secrets.
The DTSA also amends 18 U.S.C. Section 1835 to include Section 1831 (Economic Espionage) and Section 1832 (Theft of Trade Secrets) as RICO predicate acts in Section 1961(1).

This opens the door for civil RICO causes of action based upon actual offenses, “attempts to” and conspiracies to steal trade secrets by anyone (Section 1832) or by foreign governments, foreign instrumentalities or foreign agents (Section 1831).

There will now be civil [third-party] liability for foreign and domestic entities associated for association with or participation in third-party civil liability for RICO enterprises outside the “knew or had reason to know” limitations of civil trade secret law.
UTSA/DTSA: Remedies and Statute of Limitations

- Remedies are identical to the UTSA
- Statute of Limitations is identical to the UTSA: 3 years
- UTSA states: “If willful and malicious misappropriation exists, the Court may award exemplary damages in an amount not exceeding twice any award made under section (a) [compensatory] damages: actual loss/unjust enrichment
- DTSA states: “if a trade secret is willfully and maliciously misappropriated…award exemplary damages in an amount not more than 2 times the amount of [compensatory] damages
- \( X \) [compensatory] + \( 2X \) [exemplary] = treble damages
EEA/DTSA Definition of a Trade Secret

• (3) the term “trade secret” means 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 if—

• (A) the owner thereof has taken reasonable measures to keep such 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, [the public] another person who can obtain economic value from the disclosure or use of the information.

• “the public” error now fixed. Otherwise definition unchanged.
(2) "Misappropriation" means:

(i) 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

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

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

or

(B) at the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was (I) derived from or through a person who had utilized improper means to acquire it;

(II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or

(III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or

(C) before a material change of his [or her] position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.

SAME AS THE UTSA
UTSA/DTSA: Definition of “Improper Means”

• (A) "Improper means" includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means;

• [Same as the UTSA]

• But ADDS:

• (B) does not include reverse engineering, independent derivation, or any other lawful means of acquisition

• [These exceptions are already well defined in the UTSA case law].
The inevitable disclosure doctrine is still viable and still is one of the best ways to create a record to establish the “threatened” misappropriation of trade secrets.

It is NOT a cause of action.

UTSA: actual or threatened misappropriation may be enjoined.

DTSA: actual or threatened misappropriation may be enjoined BUT—an injunction cannot be based “merely on the information the person knows”

OR “conflicts with an applicable State law [California] prohibiting restraints on the practice of a lawful profession, trade or business”
Trade Secret Asset Management: The Computer/ The Internet/The Information Age

1970  Corporate assets: 80 % tangible assets/20% intangible assets

2016  Corporate assets: 20% tangible assets/80% intangible assets

Trade Secret Asset Cycle: Trade Secrets *At Rest/In Motion/In Use*

Trade Secret Situs: Intra-State, Interstate, International
Trade Secret Asset Management

• Most companies do not have any formal internal processes for trade secret assets.
• The focus has been on patents, not trade secrets, since 1982.
• Reasonable measures require processes for the identification, classification, protection and valuation of trade secret assets.
• A manual trade secret audit is time-consuming and expensive.
• The shibboleth—"we are working on it"—no longer applies.
• Companies now risk "forfeiture" of trade secret assets without pro-active steps in the 21st Century Global Economy.
The DTSA Requires Trade Secret Asset Management

• The traditional approach in trade secrets litigation under the Uniform Trade Secrets Act has been to use the liberal discovery provisions of the Federal Rules of Civil Procedure to identify, create, re-create or pronounce [for the first time] what the “trade secrets” are in the discovery phases of U.S. litigation.

• This after-the-fact approach to trade secret litigation will no longer be tolerated in the 21\textsuperscript{st} Century Economy.

• Civil law countries do even permit discovery.

• The starting point and ending point of all of trade secrets law is the “IT” analysis—what is “IT” that is alleged to be the trade secret.
The Role of Litigation in Trade Secrets Law

• Unlike patents, copyrights, and trademarks, trade secrets can only be established in court.

• No trade secret exists in law until it has been adjudicated to be a trade secret in a court of law.

• The existence of a trade secret is a question of fact to be determined by a jury.

• Therefore, a successful trade secret asset management methodology must have the goal of prevailing in court as its first priority!
Trade Secret Litigation SWAT Team

• Time is of the essence in a trade secret misappropriation lawsuit: “A trade secret once lost is lost forever.”

• Companies must development trade secret misappropriation incident response plans

• There are 8 statutory requirements for issuing an ex parte order (starting with “clearly appears”…from “specific facts”)... 

• There are 6 statutory “elements” that must be addressed in the ex parte seizure order

• There must be a “seizure hearing” not later than 7 days after the ex parte seizure order is issued.

• And exposure to damages caused by wrongful seizure!!!
The EONA Proofs

- Six proofs are required to prevail in a trade secrets litigation:
  - **Existence**
  - **Ownership**
  - **Notice**
  - **Access**
  - **Use**
  - **Damages**

- The use and damages proofs are identical to the use and damages proofs for patent and copyright.

- The EONA proofs are unique to trade secrets.
The Existence Proof: The Six-Factor Test

In 1939, the American Law Institute examined case law from the 19th and 20th Centuries and identified six factors to identify trade secret assets.

Today, this 6-factor test has become the litmus test for ascertaining whether an “information” asset qualifies as a “trade secret” asset.

The factors are not “go/no-go” tests, but factors to be considered on a sliding scale with a composite score.
Factor 1: The extent to which information is known outside the company (the more extensively the information is known outside the company, the less likely that it is a protectable trade secret).
Factor 2: The extent to which the information is known by employees and others involved in the company (the greater the number of employees who know the information, the less likely that it is a protectable trade secret).
Factor 3: How Well Secured Within Company?

**Factor 3:** The extent of measures taken by the company to guard the secrecy of the information (the greater the security measures, the more likely that it is a protectable trade secret).
Factor 4: How Important to Future Profits?

**Factor 4:** The value of the information to the company and competitors (the greater the value of the information to the company and its competitors, the more likely that it is a protectable trade secret).
Factor 5: How Much Development/Investment?

**Factor 5:** The amount of time, effort and money expended by the company in developing the information (the more time, effort and money expended in developing the information, the more likely that it is a protectable trade secret).
Factor 6: The ease or difficulty with which the information could be properly acquired or duplicated by others (the easier it is to duplicate the information, the less likely that it is a protectable trade secret).
The Defendability Factor

• The scores for the Six Factors can by mathematically combined to obtain a Defendability Factor (DF) for the trade secret.

• The Defendability Factor quantizes the extent to which the trade secret is likely to be found to meet the Existence proof in a court of law.

• The Defendability Factor allows the company to allege the misappropriation of the strongest trade secrets in any litigation, and avoid alleging weak trade secrets.

• The Defendability Factor allows the litigator to follow Sun Tzu’s admonition to choose your ground carefully.
Automated Trade Secret Asset Management: Quantifying the Six Factors

• Automated Trade Secret Asset Management is now here.
• See www.thetso.com
• Quantification on a 1-5 scale works best because everyone already knows how to grade on a one-to-five scale.
  › School grades
  › Film reviews
  › Customer surveys
• No additional employee education is required to grade the Six Factors on a one-to-five scale.
The Ownership Proof

• Does the plaintiff own the trade secret?

• Note that the “work for hire” doctrine is under the U.S. Copyright Act and does not apply to trade secrets!

• There must be an assignment from anyone involved in the creation of trade secret information to ensure the company has an ownership claim on its trade secret information.
The Notice Proof

• Have the employees been notified of what the company’s trade secrets are?

• Employees have a right to use their general knowledge, skills, and experience in future employment.

• If the employer does not draw the line between its trade secrets and the employee’s general knowledge, skills, and experience, the courts will draw that line at trial.

• Given the company’s resources, the courts will draw the line more in favor of the employee as a matter of equity.
The Access Proof

• Did the employee, in the scope of his employment, have access to the trade secret information?

• Competitors, including former employees, are free to re-invent the company’s trade secrets.

• Access to the trade secret information during his employment proves this was not a re-invention, but a misappropriation.

• Proving access depends on tracking employee exposure to trade secrets.
Classification of Trade Secrets: SFPs

• An SFP is a trade secret category: [Subject] [Format] for [Product]
  › **Subject:** the department or functional area within the company or division, such as Marketing, Engineering, Manufacturing
  › **Format:** the form of the trade secret itself, such as a method, design, plan, forecast, specification, process, device
  › **Product:** the product or family of products to which the trade secret applies
Defining the Space

• The SFPs form a three-dimensional space within which all the company’s trade secrets can be mapped
• Each trade secret lies within one SFP
SFPs - Examples

• No additional employee education is needed, because employees already use something close to this system to discuss information, we just need to formalize it.

  › Manufacturing Process for Transmissions
    – Subject Format Product
  › Research Test Results for Non-Flammable Plastics
    – Subject Format Product
  › Advertising Roll-out Strategy for New Cola
    – Subject Format Product
  › Purchasing Vendor List for MP3 Cell Phone
    – Subject Format Product
  › Software Source Code for Operating System
    – Subject Format Product
Advantages of Classification by SFP

Classification by SFP is well suited to automation. Once the possible Subjects, Formats and Products within the company have been defined, assigning each trade secret to an SFP is simply a matter of selecting the appropriate S, F, and P from three drop-down boxes. This is no more complicated than selecting the expiration month and year of your credit card for payment of an on-line purchase.

Once sorted into SFPs, the trade secrets can be managed in bundles, whether by individual SFP, or by selecting all of the trade secrets on a distinct Subject, or given Format, or relating to a specific Product or family of Products.
SFPs Eliminate the Classification Problem

The biggest problem with existing classification methods is the definition of workable criteria that encompass all the different varieties of trade secrets within the Company:

- **One Tier:** Confidential
- **Two Tier:** Highly Confidential
- **Three Tier:** Top Secret Limited Access

A large number of trade secrets means a large number of classification decisions must be made.

These classification decisions often cause confusion in litigation because an “information” asset can qualify as a “trade secret” asset *regardless of the “tier” status.*
SFPs – Classification Before Identification

• Before any specific trade secrets are identified, they can be classified and prioritized—using the Six-Factor/SFP tools.
  › Trade secrets in the same SFP are likely to share the same level of sensitivity.
  › The most valuable trade secrets will cluster within identifiable SFPs.
  › SFPs allow “triage”--the prioritization of efforts on the SFPs with the most sensitivity and the highest economic value.
This intersection is the key to trade secret asset management. In practice, trade secret audits have revealed that all of the trade secrets within a given SFP have similar six-factor scores. This means that thousands of information assets within a company can be identified and scored as trade secrets assets by ranking the SFPs, not the individual trade secrets. The importance of this in large organizations is hard to overstate.
Thank You—Questions??

- R. Mark Halligan, Esq.
- Partner FisherBroyles, LLP
- Naperville/Chicago
- (630) 200-0701
- rmarkhalligan@fisherbroyles.com
- www.fisherbroyles.com/rmarkhalligan
- Twitter: @Rmarkhalligan
- LinkedIn: https://www.linkedin.com/in/rmarkhalligan


About FisherBroyles, LLP

Founded in 2002, FisherBroyles LLP was the first national, full-service, cloud-based law firm in the country. Our Next Generation Law Firm® has grown to over 115 attorneys in 17 offices nationwide. The FisherBroyles model leverages technology to offer a more cost-effective solution to clients without sacrificing Big Law quality by eliminating unnecessary overhead that does not add value to clients.

© 2015 FisherBroyles LLP.

Disclaimer

The materials on the FisherBroyles website are for informational purposes only. They are not intended to provide legal advice for a specific situation or create an attorney-client relationship. You should not act upon the information provided on this presentation without seeking advice from a lawyer licensed in your own state or country. Under rules applicable to the professional conduct of attorneys in various jurisdictions, content on this website may be considered advertising material. The choice of a lawyer is an important decision and should not be based solely upon advertisements. Where case studies are provided, previous results are not a guarantee of similar outcomes for other clients.

Legal Notices

All text, graphics, photographs, trademarks, logos, artwork and computer code (collectively, “Content”), including but not limited to the design, structure, selection, coordination, expression, “look and feel” and arrangement of such Content, contained on this site is owned, controlled or licensed by or to FisherBroyles, LLP and is protected by trade dress, copyright, patent and trademark laws, and various other intellectual property rights.