

# Bond

IMPLICATIONS OF THE  
DEFEND TRADE SECRETS ACT OF 2016  
& PRACTICAL CONSIDERATIONS....  
WEDNESDAY, MARCH 8, 2017

## The NDNY-FCBA's CLE Committee Presents Implications of the Defend Trade Secrets Act of 2016 and Practical Considerations for Guarding Against Internal Data Theft

According to recent studies, 59% of employees admit to taking valuable company data from their employer at or around the time of termination. The cost of trade secret theft to the United States economy is staggering, with annual estimated losses between 160 to 480 billion dollars. Fortunately, on May 11, 2016, President Obama signed the Defend Trade Secrets Act of 2016 into law, thereby creating significant new protections for companies to mitigate these risks. This program will provide an overview of this important new federal law, contrast it to existing New York law, and provide practical steps that practitioners can use, including use of non-compete agreements, to protect their clients from trade secret theft.

### *Presented by*

#### **Bradley A. Hoppe**

Bradley is the chair of the Bond, Schoeneck & King's manufacturing industry group. He works with manufacturers and others to formulate strategies, strengthen policies, craft non-competition and non-disclosure agreements, and, when necessary, pursue litigation to not only protect their most important intangible assets (trade secrets, confidential information and customer relationships), but also better safeguard the products of their ingenuity and hard work from being lost to competitors through unfair and unlawful conduct.

#### **Heath J. Szymczak**

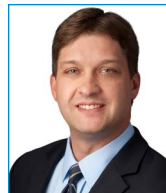
Heath has extensive litigation experience in business-related torts, complex commercial litigation, and other civil litigation, including, among other areas, contractual disputes, unfair competition claims, shareholder derivative actions, shareholder freeze-out actions, corporate valuation, breach of fiduciary duty claims, class action consumer litigation, commercial lease disputes, intellectual property disputes, healthcare network provider disputes, replevin actions, construction litigation, estates litigation, lien enforcement, products liability defense, personal injury defense, insurance fraud, and insurance coverage disputes.

Register at: <https://events.r20.constantcontact.com/register/eventR?oeidk=a07edtqs307da84f56c&oseq=&c=4deab1d0-2bad-11e3-a046-d4ae529a8250&ch=4dede620-2bad-11e3-a046-d4ae529a8250>

Attorney Advertising • © 2017 Bond, Schoeneck & King PLLC  
One Lincoln Center, Syracuse, NY 13202 • 315.218.8000



Bradley A. Hoppe  
716.416.7025  
bhoppe@bsk.com



Heath J. Szymczak  
716.416.7057  
hszymczak@bsk.com

### *Agenda*

3:15 p.m.

Registration

3:30 - 4:45 p.m.

Program

1.5 credits Professional Practice

- Introduction to Trade Secrets (15 minutes)
- Implications of Defend Trade Secrets Act of 2016 (20 minutes)
- Preventing Trade Secret Theft (20 Minutes)
- What to do in the Event of Trade Secret Theft (15 minutes)
- Questions and Answers (5 minutes)

### *Where*

*Live Presentation*

James M. Hanley Federal Building  
7th Floor Jury Assembly Room  
100 South Clinton Street  
Syracuse, New York

James T. Foley U.S. Courthouse  
*Videoconference Presentation*  
5th Floor Conference Room  
445 Broadway  
Albany, New York

 **BOND** SCHOENECK  
& KING ATTORNEYS

Commitment • Service • Value • Our Bond



**Bradley A. Hoppe**  
Member  
bhoppe@bsk.com

Buffalo, NY  
(716) 416-7025  
(716) 416-7325 fax

**Practice**  
Manufacturing

**Education**  
University of Pittsburgh  
School of Law (J.D., 2006)  
University of Pittsburgh (B.A.,  
*summa cum laude*, 2003)

**Bar/Court Admissions**  
New York  
U.S. Bankruptcy Court for the  
Western District of New York  
U.S. Court of Appeals for the  
Second Circuit  
U.S. District Court for the  
Northern District of New York  
U.S. District Court for the  
Southern District of New York  
U.S. District Court for the  
Western District of New York

## Bradley A. Hoppe

Bradley is the chair of the firm's manufacturing industry group. He works with manufacturers and others to formulate strategies, strengthen policies, craft non-competition and non-disclosure agreements, and, when necessary, pursue litigation to not only protect their most important intangible assets (trade secrets, confidential information and customer relationships), but also better safeguard the products of their ingenuity and hard work from being lost to competitors through unfair and unlawful conduct. Bradley is one of the principal architects of the firm's innovative Trade Secret Protection Audit, which utilizes a proactive approach to protect manufacturing processes, methods and systems, customer lists, and other trade secret and confidential information from both internal and external threats. He uses his extensive experience in trade secret, non-competition and related commercial litigation when necessary to protect manufacturers' and other companies' trade secret information and long-standing customer relationships in court.

Whether it be an actual or threatened misappropriation of sensitive company information, the breach of confidentiality, non-competition or non-solicitation obligations, the defense of a trade secret or unfair competition claim brought by a competitor, or any other commercial dispute, Bradley draws upon his vast litigation experience to get his manufacturing and other commercial clients the best result possible. Bradley's litigation experience includes:

- noncompete litigation
- general commercial disputes
- construction litigation
- insurance coverage disputes
- unfair competition and trade secret claims
- creditors' rights claims
- municipal defense matters
- accounting and attorney malpractice disputes
- personal injury defense

### Honors and Affiliations

- Listed in:
  - *New York Super Lawyers 2016*®, Upstate New York Rising Star, General Litigation
  - *New York Super Lawyers 2015*®, Upstate New York Rising Star, Litigation
- American Bar Association
- Bar Association of Erie County
- New York State Bar Association
- Western New York Trial Lawyer's Association
- Research Editor, *University of Pittsburgh Law Review*, 2004-2006

### Representative Publications

- Bradley A. Hoppe and Heath J. Szymczak, "A New York Litigator's Guide to the New Federal Trade Secret Law," *NY Litigator*, Fall 2016
- Heath J. Szymczak and Bradley A. Hoppe, Another Voice: Trade Secrets Act boosts Buffalo's business future, *The Buffalo News*, 5/28/16
- Bradley A. Hoppe and Heath J. Szymczak, "Head in the Cloud: The Insider Threat to a Company's Trade Secrets," *New York Law Journal*, 4/4/16



**Heath J. Szymczak**

**Member**

hszymczak@bsk.com

Buffalo, NY

(716) 416-7057

(716) 416-7357 fax

**Practice**

Litigation

**Education**

State University of New York  
at Buffalo School of Law (J.D.,  
1998)

Canisius College (M.B.A.,  
*cum laude*, 1995)

Canisius College (B.S.,  
*summa cum laude*, 1994)

**Bar/Court Admissions**

New York

U.S. Bankruptcy Court for the  
Western District of New York

U.S. District Court for the

Western District of New York

## Heath J. Szymczak

Heath has extensive litigation experience in business-related torts, complex commercial litigation, and other civil litigation, including, among other areas, contractual disputes, unfair competition claims, shareholder derivative actions, shareholder freeze-out actions, corporate valuation, breach of fiduciary duty claims, class action consumer litigation, commercial lease disputes, intellectual property disputes, healthcare network provider disputes, replevin actions, construction litigation, estates litigation, lien enforcement, products liability defense, personal injury defense, insurance fraud, and insurance coverage disputes.

### Honors and Affiliations

- Listed in:
  - *Buffalo Business First*, 2016 Legal Elite
  - *New York Super Lawyers 2016®*, Business Litigation
- New York State Bar Association, Chair, Business Torts and Employment Litigation Committee of the Torts, Insurance and Compensation Law Section (TICL); Executive Committee, TICL Section; Executive Committee, Eighth Judicial District Leader, Commercial and Federal Litigation Section; Co-Chair, Section Membership Committee; Special Committee on Discovery and Case Management in Federal Litigation; Faster, Cheaper, Smarter Working Group
- Erie County Bar Association
- American Inns of Court
- Beta Gamma Sigma Business Honor Society
- Phi Alpha Delta Law Fraternity International
- Business Editor, *Buffalo Law Review*

### Representative Presentations

- Program Co-Chair and Speaker, Implications of the Defend Trade Secrets Act of 2016 and Practical Considerations for Guarding Against Internal Data Theft, NYSBA Torts Insurance and Compensation Law Section Annual Meeting, 1/26/17

### Representative Publications

- Heath J. Szymczak and Bradley A. Hoppe, "A New York Litigator's Guide to the New Federal Trade Secret Law," *NY Litigator*, Fall 2016
- Heath J. Szymczak and Bradley A. Hoppe, "Another Voice: Trade Secrets Act boosts Buffalo's business future," *The Buffalo News*, 5/28/16
- Bradley A. Hoppe and Heath J. Szymczak, "Head in the Cloud: The Insider Threat to a Company's Trade Secrets," *New York Law Journal*, 4/4/16
- "Business Torts: A Practical Guide to Litigation," Chapter 5, *First Chair Press* 2014
- "Federal Trade Secret Legislation Moves Forward," *NYSBA Commercial and Federal Litigation Section Newsletter* - Winter 2014, Vol. 20, No. 3
- "Standardizing Efficiencies in Business Litigation," *American Bar Association Business and Torts Litigation Journal*
- "Limit Costs, Delays in Business Litigation," *Buffalo Law Journal*

### Other Activities

- Board Member, Habitat for Humanity Buffalo
- Recipient, 2010 Committee Chair of the Year, NYSBA TICL Section



**Trade Secret Theft:  
 A Growing Problem**

- Hackers
- Nation States
- Organized Crime
- Supply Chain
- Joint Venture
- Competitors
- Employees
- Accidental Disclosure



**BOND** SCHOENECK & KING ATTORNEYS

4

---

---

---

---

---

---

---

---

**How Theft is Accomplished . . . . .**

- Connecting a thumb drive to a computer
- Uploading data to the “cloud”
- Transferring data to a personal e-mail account
- 24% of employees had network access after they had left
- 82% of employers did not review what documents and data had been taken

**BOND** SCHOENECK & KING ATTORNEYS

5

---

---

---

---

---

---

---

---

**Growing Need to Protect Trade Secrets**

- Estimated **\$160 to \$480 billion** lost to trade secrets theft in U.S. each year.
- Number of trade secret cases doubled from 1995 to 2004, and are projected to double again by 2017.
- **59%** of employees admit to stealing company data after leaving. Of those, **67%** admit to using ex-employer’s data in subsequent employment

**BOND** SCHOENECK & KING ATTORNEYS

6

---

---

---

---

---

---

---

---

## Common Trade Secrets

- Formulas/recipes
- Manufacturing processes
- Business plans
- **Customer lists**
- R&D Information
- Market research, studies & analyses
- Financial Data (cost, price, margin, etc.)
- Etc.



 BOND SCHOENECK & KING ATTORNEYS

7

---

---

---

---

---

---

---

---

## Legal Framework For Protection of Trade Secrets

- NY Common Law
- Uniform Trade Secrets Act
- Computer Fraud and Abuse Act
- Economic Espionage Act
- **Defend Trade Secrets Act of 2016**

 BOND SCHOENECK & KING ATTORNEYS

8

---

---

---

---

---

---


---

---

## NY Common Law

1. Any formula, process, device, or compilation of information
2. **Used in one's business**
3. Which confers a competitive advantage over those in similar businesses
4. Who do not know it or use it.

(Restatement (First) of Torts § 757, comment b (1939))

 BOND SCHOENECK & KING ATTORNEYS

9

---

---

---

---

---

---

---

---

## Factors to Consider . . . .

1. Whether known outside the business
2. Extent known in the business;
3. Measures taken to keep secret;
4. Value to business and competitors;
5. Effort or money expended to develop; and
6. Difficulty in acquiring by others.

(Restatement (First) of Torts § 757, comment b (1939))



10

---

---

---

---

---

---

---

---

## Continuous Use

- New York rule requires that the information be “used in one’s business”
- “Continuous use” means that the alleged trade secret cannot be “information as to a single or ephemeral event in the conduct of the business”
- Could preclude protection of information pertaining to a past failed and/or abandoned secret process.



11

---

---

---

---

---

---

---

---

## Novelty and Prior Art

- Trade secret may be a device or process which is patentable; but it need not be.
- Novelty and invention are not requisite for a trade secret as they are for patentability.



12

---

---

---

---

---

---

---

---



## Misappropriation

- Under New York law, misappropriation consists of use or disclosure of a trade secret that was acquired through a relationship of trust (such as employment) or
- Through fraud or other improper means, such as theft, bribery, or hacking.



13

---

---

---

---

---

---

---

---

## Remedies

- **Injunctive Relief:** Court may order a defendant to stop violating the plaintiff's rights and to take steps to preserve the secrecy of the plaintiff's information.
- **Damages:** Court can make a defendant pay money damages to the plaintiff for the economic harm suffered. May include the plaintiff's losses resulting from the misappropriation and the defendant's profits derived from it.
- **Statute of Limitations:** The statute of limitations for a trade secret claim in New York is three years.



14

---

---

---

---

---

---

---

---

## Inevitable Disclosure Doctrine

- In New York, possible to establish irreparable harm based on the "inevitable disclosure" even in absence of non-compete.
- Key employee competes directly with former employer and had access to highly confidential information. Usually must show actual taking.
- Analogized the former employer's predicament to that of "a coach, one of whose players has left, playbook in hand, to join the opposing team before the big game."



15

---

---

---

---

---

---

---

---



## Faithless Servant Doctrine

- Grounded in the law of agency. An agent has a duty of undivided loyalty to his principal.
- If he acts adversely to employer it amounts to a fraud upon the principal so as to forfeit any right to compensation during the period of disloyalty.



16

---

---

---

---

---

---

---

---

## Uniform Trade Secrets Act

- Published by the Uniform Law Commission (the same group that brought us the Uniform Commercial Code) in 1979.
- Sought to create more predictability in the law of trade secrets for companies operating in multiple states.
- Enacted in varying forms—sometimes in whole, other times in part. New York and Massachusetts are the lone holdouts.



17

---

---

---

---

---

---

---

---

## Uniform Trade Secrets Act

- “information ... that
- (i) derives independent economic value ... 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
- (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.”

Uniform Trade Secrets Act § 1(4)



18

---

---

---

---

---

---

---

---

## Uniform Trade Secrets Act

- USTA definition is simpler. No continuous use requirement.
- Complexity and ambiguity of the New York rule leaves far more to interpretation (and litigation).
- New York rule favors innovation by limiting “squatting” on new, unpatented, technology, it also creates a loophole by permitting a competitor to benefit from another’s research and development.



19

---

---

---

---

---

---

---

---

## Computer Fraud and Abuse Act

- Permits of Federal Civil Remedy, but Limited in application.
- Access computer “without authorization”
- Obtained information relating to:
  1. “national defense or foreign relations”
  2. “financial record of a financial institution”
  3. “from any department or agency of the United States” or
  4. “from any ‘protected computer.’”



20

---

---

---

---

---

---

---

---

## “Protected Computer”

- Exclusively for the use of, or conduct that affects the use of, a financial institution or the United States Government; or
- Used in or **affecting interstate or foreign commerce or communication**, including a computer located outside United States that affects interstate or foreign commerce or communications.



21

---

---

---

---

---

---

---

---

### Economic Espionage Act

- Criminal Statute – 18 U.S.C. §§ 1831-1839.
- Previously no private civil remedy.
- Criminalizes “economic espionage” by a foreign entity as well as domestic misappropriation for financial gain.
- Notwithstanding the purpose and objectives of the EEA, its application has proven ineffective due to limited prosecutorial resources and problems with the textual limitations in the statute itself.



22

---

---

---

---

---

---

---

---

### United States v. Aleynikov

- Sergey Aleynikov - computer programmer employed by Goldman Sachs & Co.
- Left Goldman Sachs to work for another competitor. Was offered over twice his salary (\$400,000 to \$1,000,000) to develop a similar system in a fraction of the time it should take.
- Encrypted and uploaded more than 500,000 lines of source code for Goldman Sachs' computer trading system.



23

---

---

---

---

---

---

---

---

### United States v. Aleynikov

- Flew to Illinois to meet with his new employer, bringing a flash drive and a laptop containing portions of Goldman Sachs' source code with him.
- When he flew home the next day he was arrested by the FBI at Newark International Airport.



24

---

---

---

---

---

---

---

---

### United States v. Aleynikov

- Convicted under the EEA. Sentenced to 97 months of imprisonment followed by a three-year term of supervised release, and was ordered to pay a \$12,500 fine.
- Aleynikov appealed. Second Circuit reversed, finding that the source code was not “related to or included in a product that is produced for or placed in interstate or foreign commerce.”



25

---

---

---

---

---

---

---

---

## II. Implications of Defend Trade Secrets Act of 2016



26

---

---

---

---

---

---

---

---

### Background on DTSA

- Lack of uniformity and previous attempts at a uniform law (Uniform Trade Secrets Act) failed because:
  - Two major hold outs (New York and Mass)
  - Only a few states adopted all of the uniform law
  - States adopted different variations of the law
- Defend Trade Secrets Act took effect 5/11/16. Creates the first federal civil claim for trade secret theft



27

---

---

---

---

---

---

---

---

## DTSA Application

- DTSA uses the definition of “trade secret” found in the EEA, with a few slight modifications.
- “(1) In general.-- 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.**”



28

---

---

---

---

---

---

---

---

## Key Provisions of DTSA

1. Aggressive **ex parte seizure** available with respect to both the trade secret and any devices, documents or other places (e.g., servers) where it may reside in whole or in part
2. **Double damages** may be awarded
3. **Attorneys’ fees** may be awarded
4. Whistleblower immunity for anyone who discloses a trade secret under certain limited circumstances



29

---

---

---

---

---

---

---

---

## Whistleblower Immunity

- A litigant **cannot** recover double damages or attorneys’ fees unless the employee confidentiality agreement contains a whistleblower immunity provision
- “Employee” includes contractors and consultants
- “Agreement” includes any of the following:
  - Non-disclosure/confidentiality agreement
  - Non-competition/non-solicitation agreement
  - Employee handbook containing confidentiality



30

---

---

---

---

---

---

---

---

## Key Language:

“(1) Immunity.--An **individual** shall 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.”

18 U.S.C. § 1833(b)



31

---

---

---

---

---

---

---

---

## DTSA vs. New York Law

- New York law does **not** award double damages or attorneys' fees as the result of trade secret theft
- Aggressive *ex parte* seizure is **not** permitted under New York law to recover stolen trade secret information
- DTSA's definition of "trade secret" is **broader** than that recognized and applied under New York law
- Unlike New York, DTSA **rejects** "inevitable disclosure" as a basis for an injunction to prohibit employment



32

---

---

---

---

---

---

---

---

## DTSA Conclusions

- Creates more uniformity and predictability in the law for companies operating across state lines
- Provides remedies unavailable under New York law
- Requires all employment agreements and manuals with confidentiality obligations to be updated to include "whistleblower immunity notice" provisions
- Pros and cons of State vs. Federal Court



33

---

---

---

---

---

---

---

---

**DELTA FILTER CASE:  
Lessons in What Not to Do**



---

---

---

---

---

---

---

---

**DELTA FILTER:  
Lessons in What Not to Do**

- Employee was in charge of Delta's HEPA filter production.
- Employee left with another employee and started competing filter company.
- Court found that the manufacturing components of competitor's production of filters were identical to those of Delta's. BUT . . . . .

---

---

---

---

---

---

---

---

**DELTA FILTER:  
Lessons in What Not to Do**

- Court held machines could be duplicated without blueprints or photographs by simply describing them from memory (skills vs trade secret).
- Delta's president admitted that its filter production process and devices were open to inspection from time to time by representatives of its competitors.

---

---

---

---

---

---


---

---



**DELTA FILTER:  
Lessons in What Not to Do**

- “[I]n the absence of any secrecy agreement preventing defendants from using the technical knowledge which they naturally and legitimately acquired during their employment, the credible evidence does not support any inference that they used improper means to acquire the information . . . or that such means were necessary to do so.”

 37

---

---

---

---

---


---


---

---

**DELTA FILTER:  
Lessons in What Not to Do**

- “[T]he actions . . . were ‘as consistent with the normally expected desire for fair, economic self-improvement as they [were] with a well-planned, well-concealed conspiratorial attempt at industrial piracy.’”



 38

—  
—

---

---

---

---

---

---

---

---

**III. Theft Prevention:  
The Trade Secret  
Audit**

 39

---

---

---

---

---

---

---

---

**A Trade Secret Audit:**

1. Identify Trade Secrets and Threats
2. Review Agreements
3. Review Onboard Protocol
4. Review Physical Security
5. Review Digital Security
6. Review Departure & Theft Protocols
7. Develop Culture of Protection



**BOND SCHOENECK & KING ATTORNEYS**

40

---

---

---

---

---

---

---

---

- Memorialize the Company's Secrecy Policy
- Restrict Internal Access to Trade Secrets
- Limit/Eliminate Access to the "cloud"
- Physical Security - Lock Cabinets
- Label Trade Secret Documents
- Maintain Computer Secrecy
- Restrict Public Accessibility
- Deal Cautiously with Third Parties:  
Use Contracts



**BOND SCHOENECK & KING ATTORNEYS**

41

---

---

---

---

---

---

---

---

**Contracts: Restrictive Covenants**

1. Non-Compete
2. Non-Solicit
3. Non-Disclosure/Confidentiality



**BOND SCHOENECK & KING ATTORNEYS**

42

---

---

---

---

---

---

---

---

## Restrictive Covenants

- Protect trade secrets/confidential information
- Protect goodwill and customer relationships
- Provide means to seek certain types of relief:
  - Defend Trade Secrets Act double damages
  - Return of compensation paid
  - Attorneys' fees and costs
  - Injunctive relief



43

---

---

---

---

---

---

---

---

---

---

## Restrictive Covenants – Standard

1. Sufficient consideration is a must ...
  - Initial employment
  - Continued employment\*
  - Promotion
  - Severance benefits
  - Termination “for cause” vs. “without cause”

More is not better: you cannot “buy” longer or broader covenants with more consideration

\* Zellner v. Stephen D. Conrad, M.D., P.C., 183 A.D.2d 250 (2d Dept. 1992)



44

---

---

---

---

---

---

---

---

---

---

## Restrictive Covenants – Standard Termination “For Cause” vs. “Without Cause”

- Until recently, it was understood that a non-compete was unenforceable if employee terminated without cause.\*
- The Fourth Department\*\* held otherwise in 2014
  - Distinguished between “non-compete” and “forfeiture for competition” clauses and limited *Post, supra* to the latter.
  - Held that a without cause termination “would not render a non-compete unenforceable,” but was a relevant factor in balancing the equity for purposes of a preliminary injunction.
  - The Court of Appeals later reversed *Brown & Brown* on other grounds, but did not overrule the without cause determination.

\* *Post v. Merrill Lynch, Pierce, Fenner & Smith, Inc.*, 48 N.Y.2d 84 (1979) (finding a “forfeiture for competition” provision unenforceable where employee terminated without cause).

\*\* *Brown & Brown, Inc. v. Johnson*, 115 A.D.3d 162 (4th Dept. 2014).



45

---

---

---

---

---

---

---

---

---

---

## Restrictive Covenants – Standard

### Termination “For Cause” vs. “Without Cause”

- The First Department\* rejected the Fourth Department’s holding in November of 2016.
  - Relied upon *Post, supra* to hold a non-compete unenforceable where “the employer ... does not demonstrate ‘continued willingness to employ the part covenanting not to complete.’”
  - Ignored *Brown & Brown, supra* and made no attempt to distinguish between “non-compete” and “forfeiture for competition” clauses.
- For practitioners in the First and Fourth Departments, this seems to be a settled issue, but for everyone else ...

\* *Buchanan Capital Mkts., LLC v. DeLucca*, 144 A.D.3d 508 (1st Dept. 2016).

---

---

---

---

---

---

---

---

---

---

## Restrictive Covenants – Standard

2. Must be reasonable in time and area and no broader than necessary to protect legitimate interests, and cannot be harmful to the public and/or impose an undue burden\*

- 2 years generally enforceable
- Area depends on footprint of business/employee
- Legitimate interests include:
  - Trade secrets
  - Goodwill/customer relationships
  - Key employees
- The covenant cannot violate New York public policy

\* See, e.g., *BDO Seidman v. Hirshberg*, 93 N.Y.2d 382 (1999)

---

---

---

---

---

---

---

---

---

---

## Consequences of Overbreadth

If you are lucky, then the Court will strike only the overbroad portion and enforce the remainder of the covenant




---

---

---

---

---

---

---

---

---

---

## Consequences of Overbreadth

If unlucky, then the nightmare scenario exists: the Court will strike the **entire** provision potentially leaving your trade secrets and customer relationships exposed.



49

---

---

---

---

---

---

---

---

## *Brown & Brown, Inc. v. Johnson*, 115 A.D.3d 162 (4<sup>th</sup> Dept. 2014)

- Analyzed employment agreement containing customer non-solicitation and Florida choice of law provisions
- Invalidated choice of law provision because Florida law was "truly obnoxious" to New York public policy
- Held that a "without cause" termination did not render the non-solicitation provision unenforceable
- Held that the non-solicitation was overbroad because it applied to **all** customers instead of those **customers with whom employee developed relationships**



50

---

---

---

---

---

---

---

---

## *Brown & Brown, Inc. v. Johnson*, 115 A.D.3d 162 (4<sup>th</sup> Dept. 2014)

- The court analyzed whether the customer non-solicitation provision should be partially enforced.
- The standard: the **employer** must establish "an absence of overreaching, coercive use of dominant bargaining power, or other anti-competitive misconduct [and that it acted] in good faith [] to protect a legitimate business interest, consistent with reasonable standards of fair dealing."



51

---

---

---

---

---

---

---

---

*Brown & Brown, Inc. v. Johnson,*  
115 A.D.3d 162 (4<sup>th</sup> Dept. 2014)

- Employer failed to satisfy standard because:
  - The court found that the employer waited until the first day of employment before notifying defendant of the agreement and only after the defendant quit her prior employment
  - The employer presented the agreement to defendant after *BDO Seidman*, so it was on notice of the overbreadth
  - The employer included a partial enforcement provision in the agreement in an attempt to escape *BDO Seidman*
- Court thus invalidated the entire covenant



52

---

---

---

---

---

---

---

---

---

---

*Brown & Brown, Inc. v. Johnson,* 25  
N.Y.3d 364 (2015)

- Court affirmed in part and reversed in part.
- Affirmed that part of the decision finding that Florida law was “truly obnoxious” to New York public policy.
- Did not disturb the finding that a “without cause” termination does not invalidate the covenant.
- Reversed the partial enforcement finding because questions of fact existed surrounding defendant’s hire and the notice provided of the agreement.



53

---

---

---

---

---

---

---

---

---

---

*Brown & Brown, Inc. v. Johnson*  
Conclusion

- The Court of Appeals remanded the case to the trial court to determine partial enforcement
- The trial court ultimately found, after a bench trial, that the employer failed to satisfy its burden for partial enforcement of the covenant.
- After appeals to the Fourth Department and the Court of Appeals, a bench trial, and likely **hundred of thousands of dollars spent**, the non-solicitation provision was completely invalidated.



54

---

---

---

---

---

---

---

---

---

---

Don't Panic: It Can Still Be Fixed

- Periodic reviews/updates essential
- Covenants can be updated as part of:
  - Continued employment
  - Promotion
  - Other positive change in employment
  - Severance benefits



55

---

---

---

---

---

---

---

---

**IV. Theft Mitigation:  
What to Do in the  
Event of Theft**



56

---

---

---

---

---

---

---

---

What To Do In The Event of a Theft?

**1. Contact an attorney.**

**A victim of trade secret theft needs someone with expertise in this area who can walk him/her through all of the steps necessary to preserve and obtain relevant information/evidence and better protect his/her rights in future litigation.**



57

---

---

---

---

---

---

---

---



## What To Do In The Event of a Theft?

### 2. Ensure that all devices are preserved.

- Computer, laptops, smart phones, tablets, thumb drives, hard drives, etc. must be set aside in a secure place so that important evidence is not lost.
- Do not put devices back into circulation. This will compromise the data, destroy chain of custody and negatively impact a client's ability to prove its case.



58

---

---

---

---

---

---

---

---

## What To Do In The Event of a Theft?

### 3. Ensure that all emails and other data are preserved.

At a minimum, you need to:

- Identify all employees with relevant information and issue preservation instructions and disable the auto-delete function on their computers and any other relevant devices; and
- Confirm that backup tapes are performing properly



59

---

---

---

---

---

---

---

---

## What To Do In The Event of a Theft?

### 4. Cut off ex-employee's access to trade secrets

- Server
- Cloud accounts
- Access to physical files

### 5. Photograph and take inventory of work space

### 6. Interview and review emails of other employees



60

---

---

---

---

---

---

---

---

## What To Do In The Event of a Theft?

All of these steps need to be taken ASAP to:

- Identify exactly what has been taken.
- Identify if anyone else is involved.
- Mitigate damage by preventing future theft
- Establish that you have taken reasonable steps to protect your information and your company, which is essential to obtaining injunctive relief in Court



61

---

---

---

---

---

---

---

---

## Questions?



62

---

---

---

---

---

---

---

---

## Thank You!



63

---

---

---

---

---

---

---

---

# A NEW YORK LITIGATOR'S GUIDE TO THE NEW FEDERAL TRADE SECRET LAW<sup>1</sup>

By Heath J. Szymczak and Bradley A. Hoppe<sup>2</sup>

## I. Introduction

On May 11, 2016, President Barack Obama signed into law the Defend Trade Secrets Act of 2016 ("DTSA"), creating the first federal civil claim for theft of trade secrets. This is one of the most significant developments in trade secret law in decades. Prior to DTSA, trade secrets did not receive the same protections afforded to other forms of intellectual property such as trademarks, copyrights, and patents. DTSA elevates the status of trade secrets to the point where its remedies, in many instances, now exceed those which may have been previously available under state law, including aggressive ex parte seizure mechanisms (similar to those used to seize counterfeit goods under trademark law), exemplary damages, and attorney's fees.

Trade secret misappropriation was previously governed by state law, with almost all other states adopting various versions of the Uniform Trade Secrets Act ("UTSA").<sup>3</sup> New York is one of the last states that have refused to adopt UTSA. The passage of DTSA thus has significant implications for a commercial litigator in New York, as he/she, for the first time, will have available to him/her a statutory framework for enforcement of trade secrets.<sup>4</sup>

DTSA is a civil amendment to the Economic Espionage Act of 1996, ("EEA"), a criminal statute.<sup>5</sup> The EEA makes it a federal criminal offense to misappropriate a trade secret that is linked to interstate or foreign commerce. The EEA, however, did not provide for a private right of action in federal court. Instead, trade secret owners seeking protection under the EEA had to stand in line and hope for investigation and prosecution by an already over-extended Federal Bureau of Investigation and Department of Justice. Consequently, prosecutions under the EEA have been limited

---

<sup>1</sup> This article was published in the New York State Bar Association's *NY Litigator* - Fall 2016 (Vol. 21, No. 2).

<sup>2</sup> Heath J. Szymczak and Bradley A. Hoppe are members in Bond Schoeneck & King, PLLC's Litigation Department and have extensive experience in protecting companies from trade secret theft, particularly from former employees. Messrs. Hoppe and Szymczak have developed an innovative Trade Secret Protection Audit which systematically reviews a company's agreements, policies and protocols, as well as their physical and electronic security measures.

<sup>3</sup> UTSA has been adopted in 48 States and the District of Columbia, but not in New York or Massachusetts. See "*Uniform Law Commission: The National Conference of Commissioners on Uniform State Laws, Uniform Trade Secrets Act*", available at <http://www.uniformlaws.org/Act.aspx?title=Trade+Secrets+Act>.

<sup>4</sup> The authors forecasted the passage of DTSA in the Commercial and Federal Litigation Section's Newsletter, Winter 2014, Vol. 20, No. 3, page 7, "*Federal Trade Secret Legislation Moves Forward*," available at <http://www.nysba.org/WorkArea/DownloadAsset.aspx?id=54068>.

<sup>5</sup> 18 U.S.C. §§ 1831 et seq.

and have not provided an effective deterrent to trade secret theft.<sup>6</sup> By providing trade secret owners with direct access to federal courts through a mechanism to vindicate private rights, together with robust remedial provisions, DTSA is designed to create a greater deterrent to trade secret theft than previously existed at the federal level.

The purpose of this article is to provide New York commercial litigators, who may be unfamiliar with UTSA and the EEA, with an understanding of the background and context from which DTSA evolved, as well as a clearer picture of the scope of DTSA generally and how federal courts are likely to construe its provisions specifically. The reader will gain an understating of why DTSA was enacted and how it is different from and broader than both New York law and UTSA. Specifically, this article will provide: (1) a comparison of New York Law and UTSA; (2) a description of the EEA and New York's *Aleynikov* case and how that led to DTSA's enactment; (3) a description of the procedural background and evolution of DTSA; and (4) a summary of DTSA's key provisions and how they are likely to be interpreted.

## II. Comparison of New York Law and UTSA

DTSA draws significantly from UTSA and was designed, in part, to provide a mechanism for greater state-to-state uniformity, albeit an incomplete one.<sup>7</sup> As such, an understanding of UTSA is important in approaching DTSA, particularly for a litigator in New York where UTSA has never been adopted.

UTSA was originally published by the Uniform Law Commission (the same group that brought us the Uniform Commercial Code) in 1979, and later amended in 1985, for the purpose of providing a uniform act throughout the United States to create more predictability in the law of trade secrets for companies operating in multiple states. UTSA has since been enacted in varying forms—sometimes in whole, other times in part and, still others, with material changes to reflect certain aspects of a particular state's common law. As noted, New York and Massachusetts are the lone holdouts.

While there has been a recent push in New York (as well as Massachusetts) to enact some form of UTSA,<sup>8</sup> New York courts continue to rely upon and apply highly developed, albeit often complex, common law rules for trade secret protection. As

---

<sup>6</sup> See, "Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?: Hearing Before the Senate Judiciary Comm., Subcomm. on Crime and Terrorism," 113th Cong. (2014) (statement of Randall C. Coleman, Assistant Director, Counterintelligence Division, FBI); see also Robin L. Kuntz, "How Not to Catch a Thief: Why the Economic Espionage Act Fails to Protect American Trade Secrets," 28 Berkeley Technology Law Journal Issue 4 (2013).

<sup>7</sup> As discussed below, DTSA does not expressly preempt USTA.

<sup>8</sup> New York is currently considering a bill, Senate Bill 3770, to adopt UTSA without significant modifications. It is currently in committee. See, <https://www.nysenate.gov/legislation/bills/2015/s3770>. Massachusetts has also recently moved closer to adopting UTSA. Massachusetts House Bill H4434, which adopts UTSA, unanimously passed the House and was transmitted to the Senate Rules Committee. See "Massachusetts Senate Votes for Tough Noncompete Bill and Adoption of Uniform Trade Secrets Act," (July 14, 2016), available at <https://faircompetitionlaw.com/2016/07/14/massachusetts-senate-votes-for-tough-noncompete-bill-and-adoption-of-uniform-trade-secrets-act/>.

explained below, UTSA is in many respects broader than the common law, both in terms of the protections afforded and the remedies provided to litigant victims of trade secret theft.

With respect to the scope of the protections afforded under UTSA, a trade secret is defined more broadly and with far less complexity than its common law counterpart. Specifically, New York common law defines a trade secret as any “formula, pattern, device or compilation of information which is used in one’s business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it” and then applies the following six factor balancing test to determine whether the information meets the definition:

(1) the extent to which the information is known outside of the business; (2) the extent to which it is known by employees and others involved in the business; (3) the extent of measures taken by the business to guard the secrecy of the information; (4) the value of the information to the business and its competitors; (5) the amount of effort or money expended by the business in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.<sup>9</sup>

UTSA, on the other hand, applies a far simpler definition and test for trade secret protection by defining a “trade secret” as “information ... that (i) derives independent economic value ... 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** (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.”<sup>10</sup> While the purpose of the two definitions/rules are obviously the same (i.e., to protect information of value that is secret from competitors), the complexity and ambiguity of the New York rule leaves far more to interpretation (and litigation). While the New York rule may be good for litigators, such is often not the case for clients, as it leads to increased litigation costs and interjects greater uncertainty into the predictability of outcomes for business transactions and relations.

In addition, the New York rule, unlike UTSA, requires that the information be actually “used in one’s business,”<sup>11</sup> which has been construed as a “continuous use” requirement for trade secret protection.<sup>12</sup> While courts have clarified that “continuous use” means only that the alleged trade secret cannot be “information as to a single or

---

<sup>9</sup> *Ashland Management v. Janien*, 82 N.Y.2d 395, 407 (1993) (quoting Section 757 of the Restatement of Torts, comment b).

<sup>10</sup> Uniform Trade Secrets Act § 1(4) (emphasis added).

<sup>11</sup> *Janien*, 82 N.Y.2d at 407.

<sup>12</sup> See, e.g., *Lehman v. Dow Jones & Co.*, 783 F.2d 285, 297-298 (2d Cir. 1986).

ephemeral event[] in the conduct of the business,”<sup>13</sup> the fact remains that this requirement would seemingly preclude protection of information pertaining to a past failed and/or abandoned secret process or formula that could nevertheless have economic value to a competitor. The rule under UTSA, on the other hand, is significantly broader in this respect and provides trade secret protection to any secret information, currently in use or long since abandoned, which derives any economic value.<sup>14</sup> While one could argue that the New York rule favors innovation by disincentivizing a company from squatting on new, unpatented, technology, it also creates a loophole of sorts in the law by seemingly permitting a competitor to reap the benefits of another company’s valuable research and development.

Not only does UTSA expand the scope of trade secret protection afforded by the common law, but it also provides additional remedies not otherwise available. For example, in the event that a UTSA plaintiff can establish that a defendant’s misappropriation was willful or malicious, or if a defendant can establish that a plaintiff’s claim was made in bad faith, the statute provides for attorneys’ fees to the prevailing party.<sup>15</sup> Similarly, a plaintiff who establishes that a defendant’s misappropriation was willful or malicious may be awarded “exemplary damages in an amount not to exceed twice any [damage] award” for actual loss.<sup>16</sup> Under the common law, a litigant is, of course, only entitled to its actual damages for any losses sustained and, in the absence of extraordinary circumstances or a “prevailing party” attorneys’ fees provision in an employment or other contract, will not be awarded any attorneys’ fees incurred in the litigation.

Finally, unlike New York law where an injunction prohibiting employment on the basis of “inevitable disclosure” is, at best, on shaky ground,<sup>17</sup> there exists a significant body of case law standing for the proposition that UTSA permits (and, in essence, codifies) “inevitable disclosure” to enjoin an employee from taking employment with a competitor.<sup>18</sup> While criticized by some other courts,<sup>19</sup> the fact that UTSA permits injunctive relief based upon both “actual and **threatened** misappropriation”<sup>20</sup> has given far more traction and credibility to the applicability of the “inevitable disclosure” to prohibit employment than what currently exists under New York law.

While UTSA affords broader protection to trade secrets and provides greater remedies to litigants than what exists under the common law, it has largely failed in its stated

---

<sup>13</sup> *Id.*; see also, *Zylon Corp. v Medtronic, Inc.*, 2015 N.Y. Misc. LEXIS 1276 (N.Y. Co. Sup. Ct. 2015).

<sup>14</sup> Uniform Trade Secrets Act § 1(4).

<sup>15</sup> Uniform Trade Secrets Act § 4.

<sup>16</sup> Uniform Trade Secrets Act § 3(b).

<sup>17</sup> See, e.g., *Janus et Cie v. Kahnke*, 2013 U.S. Dist. LEXIS 139686 (S.D.N.Y. 2013) (rejecting claim of inevitable disclosure in the absence of a noncompete or evidence of actual misappropriation).

<sup>18</sup> *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262 (7th Cir. 1995).

<sup>19</sup> *Kelly Services v. Greene*, 535 F.Supp. 2d 180, 188 (D. Me. 2008) (rejecting argument that the MUTSA (Michigan Uniform Trade Secrets Act) permits an injunction based on “inevitable disclosure”).

<sup>20</sup> Uniform Trade Secrets Act § 2(a) (emphasis added).

purpose of providing uniformity and predictability for trade secrets across state lines, as there remain two major hold outs (New York and Massachusetts) and numerous states which have adopted only variations of the “uniform” statute. As discussed below, DTSA, which is modeled after UTSA, goes a step further than UTSA by not only creating a federal civil claim for trade secret misappropriation on par with other intellectual property rights, but also providing greater protection and remedies than what exists under UTSA.

### III. EEA, New York’s *Aleynikov* Case, and DTSA

Given the lack of uniformity in trade secret law across state lines, DTSA was partly designed to provide an overarching umbrella statute to UTSA. More directly, however, DTSA was aimed at the limitations of the EEA by expressly amending that statute. Thus, an understanding of the EEA is also important since a New York commercial litigator may not have had much- if any - exposure to this federal criminal statute either.<sup>21</sup>

The EEA criminalizes “economic espionage” by a foreign<sup>22</sup> entity as well as domestic misappropriation for financial gain.<sup>23</sup> Notwithstanding the purpose and objectives of the EEA, its application has proven ineffective due to limited prosecutorial resources and problems with the textual limitations in the statute itself.

For example, the New York case of *United States v. Aleynikov*<sup>24</sup> exposed major holes in the EEA and the ability of the government to prosecute claims for trade secret theft. In *Aleynikov*, Sergey Aleynikov was a computer programmer employed by Goldman Sachs & Co. to develop computer source code for the company’s trading system.<sup>25</sup> Aleynikov left Goldman Sachs to work for another company looking to develop a similar computer system.<sup>26</sup> He was offered over twice his salary (\$400,000 to \$1,000,000) to develop a similar system in a fraction of the time that it would usually take to develop such a system.<sup>27</sup>

---

<sup>21</sup> Some New York litigators may be familiar with the federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030, which does provide a private right of action. However, that statute is fairly limited in application to cases involving computers of the federal government or certain financial institutions or where the crime is interstate in nature. The statute is more commonly aimed at computer “hacking” rather than directly at theft of trade secrets (which also do not always reside on a computer). It is usually difficult to apply this statute to situations where an employee (such as in the *Aleynikov* case discussed below) accesses his employer’s computer in the process of uploading trade secret data since the access to the computer itself was not necessarily “unauthorized.”

<sup>22</sup> See, 18 U.S.C. § 1831(a).

<sup>23</sup> See, 18 U.S.C. § 1832(a).

<sup>24</sup> *United States v. Aleynikov*, 676 F3d 71 (2d Cir. 2012).

<sup>25</sup> *Id.* at 74.

<sup>26</sup> *Id.*

<sup>27</sup> *Id.*



On his last day at Goldman Sachs, Aleynikov encrypted and uploaded more than 500,000 lines of source code for Goldman Sachs' computer trading system.<sup>28</sup> After uploading the source code, Aleynikov deleted the history of his computer commands.<sup>29</sup> When he returned to his home in New Jersey, Aleynikov downloaded the source code from a remote server in Germany to his home computer.<sup>30</sup> Aleynikov then flew to Illinois to meet with his new employer, bringing a flash drive and a laptop containing portions of Goldman Sachs' source code with him.<sup>31</sup> When he flew home the next day he was arrested by the FBI at Newark International Airport.<sup>32</sup>

Following a jury trial in the United States District Court for the Southern District of New York, Aleynikov was convicted under Section 1832 of the EEA.<sup>33</sup> He was sentenced to 97 months of imprisonment followed by a three-year term of supervised release, and was ordered to pay a \$12,500 fine. Aleynikov appealed. On April 11, 2012, the Second Circuit reversed Aleynikov's conviction, finding that his conduct did not constitute an offense under the EEA because the source code was not "related to or included in a product that is produced for or placed in interstate or foreign commerce," thus significantly undermining and weakening the EEA's ability to deter misappropriation of valuable trade secrets.<sup>34</sup>

In December 18, 2012, Congress amended the EEA to try to close the "Aleynikov loophole" in a law referred to as the "Theft of trade secrets clarification act of 2012."<sup>35</sup> That same year Congress also began working toward the creation of a federal civil claim for misappropriation of trade secrets. In 2012, Senators Herb Kohl, Christopher Coons, and Sheldon Whitehouse introduced without success the "Protecting American Trade Secrets and Innovation Act of 2012" in the 112th Congress. In 2014, a new bipartisan bill was introduced in the Senate by Senators Christopher Coons and Orrin

---

<sup>28</sup> *Id.*

<sup>29</sup> *Id.*

<sup>30</sup> *Id.*

<sup>31</sup> *Id.*

<sup>32</sup> *Id.*

<sup>33</sup> Aleynikov was charged with violating 18 U.S.C. § 1832 (trade secret theft), not § 1831 (economic espionage).

<sup>34</sup> *Id.* at 74. 18 U.S.C. § 1832 (trade secret theft) imposes a limitation not found in § 1831 (economic espionage): "Whoever, with intent to convert a trade secret, that is related to or included in a product that is **produced for or placed 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, knowingly ... without authorization ... downloads, uploads, ... transmits, ... or conveys such information" is guilty of a federal offense, and may be imprisoned for up to 10 years. *Id.* § 1832(a) (emphasis added). The court Second Circuit found that evidence of this limitation was lacking with respect to the source code.

<sup>35</sup> S. 3642 (112<sup>th</sup> Congress). Aleynikov would subsequently be prosecuted under state law, which would continue for several years, and also ultimately fail. Litigation continues over payment Aleynikov's legal fees, with a decision as recently as July 13, 2016. See *Jef Feeley "Goldman Sachs Wins Fight Over Ex-Programmer's Legal Fees,"* available at <http://www.bloomberg.com/news/articles/2016-07-13/former-goldman-sachs-programmer-loses-fight-over-legal-fees>.

Hatch in the 113th Congress, entitled “Defend Trade Secrets Act of 2014.” An identical textual bill was also introduced in the House by Congressman George Holding, though under the name “Trade Secret Protection Act of 2014”. While the Senate bill stalled, the House bill was unanimously passed by the House Judiciary Committee on September 17, 2014, but failed to come to the floor for a vote.

Finally, in July of 2015, identical textual bills were introduced simultaneously in the 114th Congress. This time both bills were entitled “Defend Trade Secrets Act of 2015.” The House bill was introduced by Congressman Doug Collins. The Senate Bill was once again introduced by Senator Hatch. The 2015 version contained several modifications to the 2014 version in order to make it more palatable to past critics and bring it more in line with UTSA.<sup>36</sup> On April 4, 2016, the U.S. Senate passed the legislation with a unanimous vote of 87-0. On April 27, 2016, DTSA was approved by the U.S. House of Representatives by a vote of 410-2. As noted, President Obama signed DTSA into law on May 11, 2016.

#### IV. DTSA’s Key Provisions

##### a. Definition of “Trade Secret”

With the background and context of DTSA explained, we now turn to the key provisions of DTSA itself. In particular, DTSA uses the definition of “trade secret” found in the EEA, with a few slight modifications, as shown below:

(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; and~~ **another person who can obtain economic value from the disclosure or use of the information . . . .**<sup>37</sup>

---

<sup>36</sup> See, Substitute Amendment EHF16041 and Leahy-Grassley Amendment ALB16037.

<sup>37</sup> See 18 U.S.C. § 1839 (3) and (4); 114 P.L. 153, 130 Stat. 376 at 380-381 (deletions shown by strikethrough and additions shown in bold).

As noted above, DTSA's definition tracks the most widely used state definitions under USTA,<sup>38</sup> and, significantly, is broader than the definition currently available under New York law.<sup>39</sup> The additional language added by the amendment (in bold) also creates greater protection by restricting the scope of trade secret discovery (and resulting loss of status) from the "public" in general to a smaller class which is essentially limited to competitors, bringing DTSA in closer conformity with USTA than exists under the EEA.<sup>40</sup>

"Misappropriation" may be established by showing acquisition of the trade secret by "improper means" or disclosure or use of the same where the person in possession of the trade secret (1) knew or should have known that the information was acquired by improper means or under circumstances giving rise to a duty of secrecy, or (2) prior to making a material change in position, the person in possession knew or should have known that the trade secret was disclosed by accident or mistake.<sup>41</sup> As under UTSA, "wrongful means" under DTSA includes theft, bribery, misrepresentation, breach, or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means. However, reverse engineering and independent derivation of the trade secret do not constitute improper means.<sup>42</sup>

#### **b. Ex Parte Seizure**

One of the most controversial aspects of DTSA, and a remedy not found in UTSA, is its allowance for a trade secret owner to seek ex parte seizure of trade secret materials under "extraordinary circumstances."<sup>43</sup> In order to obtain such an order, however, several onerous requirements must be met. As a preliminary matter, a court will not issue such an order unless the applicant meets the threshold requirement for issuance of an injunction, including irreparable injury and a balancing of the equities, as well as a finding by the court that an order issued pursuant to Rule 65 of the Federal Rules of Civil Procedure or another form of equitable relief would be inadequate because the party to which the order would be issued would evade, avoid, or otherwise not comply with such an order.

The applicant must then also show a likelihood of success in establishing that (1) the information is a trade secret; (2) the person against whom seizure would be ordered misappropriated the trade secret of the applicant by improper means (or conspired to do

---

<sup>38</sup> The language of the proposed Section 279-N(D) of the UTSA bill currently pending in New York (S.3770), proposed new Article 17-B of the New York Business Corporation Law, is nearly identical.

<sup>39</sup> See, Restatement of Torts §757, requiring actual and continuous use.

<sup>40</sup> Both the Court of Appeals for the Seventh Circuit, in *United States v. Lange*, 312 F.3d 263, 267 (7th Cir. 2002), and the Court of Appeals for the Third Circuit, in *United States v. Hsu*, 155 F.3d 189, 196 (3d Cir. 1998), have identified the potential significance of this difference between UTSA and the EEA. The Senate Judiciary Committee noted that it did not intend for DTSA definition of a trade secret to be meaningfully different from that generally used in states that have adopted UTSA.

<sup>41</sup> 114 P.L. 153, 130 Stat. at 381. "Misappropriation" and "improper means" are also defined identically to the definitions used by most states under UTSA.

<sup>42</sup> *Id.*

<sup>43</sup> *Id.* at 376.

so); and (3) the person against whom seizure would be ordered has actual possession of the trade secret (described with reasonable particularity) and that the order is needed to prevent dissemination of the trade secret (which could render the trade secret without value). The applicant must also show that he has not publicized the requested seizure.<sup>44</sup> These requirements are similar to, but slightly more rigorous than, a showing required for the seizure of counterfeit goods under trademark law (i.e. the Trademark Act of 1946 or the Lanham Act).<sup>45</sup>

DTSA also provides detailed requirements for what a seizure order must contain, including: (1) mandates for narrowly tailored seizures; (2) reasonable steps to avoid interruption of the business of third parties, as well as the defendant's legitimate business operations; (3) guidance to law enforcement on how to proceed in effecting the seizure; (4) a prompt hearing date following the order's issuance; (5) protection of the seized material; and (6) posting of a bond on the part of the petitioning party. A court must take custody of any seized materials and hold a seizure hearing within seven days. An interested party may file a motion to encrypt seized material. A party harmed by a wrongful or excessive seizure may move to dissolve or modify the order and may also seek relief against the applicant of the seizure order for any resulting losses.<sup>46</sup>

### **c. Damages (Including Exemplary Damages and Attorney's Fees)**

DTSA allows for an award of damages for actual loss caused by the misappropriation of the trade secret, as well as damages for any unjust enrichment that is not addressed in computing damages for actual loss. In lieu of damages measured by any other methods, DTSA also permits for damages to be measured in terms of the imposition of a reasonable royalty for the defendant's unauthorized disclosure or use of the trade secret. Moreover, and most importantly for litigators and clients alike, if a plaintiff is able to show that the trade secret was "willfully and maliciously misappropriated," a court may award exemplary damages in "an amount not more than 2 times the amount of the damages awarded."<sup>47</sup> Finally, if (1) a claim of misappropriation is made in bad faith, (2) a motion to terminate an injunction is made or opposed in bad faith, or (3) the trade secret was willfully and maliciously misappropriated, a court may disregard the American rule for attorney's fees and award reasonable attorney's fees to the prevailing party.<sup>48</sup>

### **d. "Inevitable Disclosure Doctrine" Not Adopted**

DTSA specifically states that an injunction issued thereunder cannot "prevent a person from entering into an employment relationship" and that any conditions placed on such

---

<sup>44</sup> *Id.* at 376-377.

<sup>45</sup> See, Section 34 of the Lanham Act, 15 U.S.C. § 1116(d)(4)(B).

<sup>46</sup> 114 P.L. 153, 130 Stat. at 377-379.

<sup>47</sup> A treble damages provision was included in the 2014 version of DTSA but was replaced with a double damages provision in the 2015/2016 version adopted.

<sup>48</sup> *Id.* at 379-380.

a relationship must be based on more than "the information the [former employee] knows[.]"<sup>49</sup> Thus, DTSA makes clear that the "inevitable disclosure doctrine" will not apply in any circumstances under the statute. This doctrine, which exists under New York law, albeit on shaky ground, allows an employer to restrain a former employee from working for a competitor (at least temporarily) based on a showing that the former employee's knowledge of the employer's critical proprietary information is so comprehensive that the employer's trade secrets would inevitably be disclosed and used in the course of the former employee's new employment.<sup>50</sup> Needless to say, the clear language in DTSA would preclude a New York litigant from pursuing such an argument under the terms of the statute. This is not to say, however, that a litigant cannot seek an injunction with respect to the "conditions placed on such employment" (such as not contacting customers the employee dealt with), though the scope and breadth of such conditions and restrictions will necessarily be fleshed out by the courts, hopefully in the near future.

#### **e. Whistleblower Immunity Notice Requirement**

Imbedded within the text of DTSA is a warning that a plaintiff will not be able to recover exemplary damages or attorney fees if it fails to include a "whistleblower immunity notice" in "any contract or agreement with an employee that governs the use of a trade secret or other confidential information," such as non-disclosure, non-solicitation, and non-competition agreements.<sup>51</sup> The notice must inform the employee (among other things) that he or she cannot be held liable under any trade secret law for the disclosure of a trade secret that is made (1) in confidence to a government official or to an attorney for the sole purpose of reporting a suspected violation of law or (2) in a document in a lawsuit or proceeding filed under seal.<sup>52</sup>

DTSA further provides, however, that an "employer shall be considered to be in compliance with the notice requirement . . . if the employer provides a cross-reference to a policy document provided to the employee that sets forth the employer's reporting policy for a suspected violation of law."<sup>53</sup> Significantly, this notice requirement also may extend to individuals who are independent contractors performing work for a company, as DTSA defines an "employee" to include "any individual performing work as a contractor or consultant for an employer."<sup>54</sup> The notice, however, appears to only be required with "individuals" and may not be required for a third-party company in a joint venture non-disclosure agreement or other such agreement.

---

<sup>49</sup> *Id.*

<sup>50</sup> *See, Willis of N.Y., Inc. v. DeFelice*, 299 A.D.2d 240, 242, 750 N.Y.S.2d 39 (1st Dept. 2002)(citing *EarthWeb, Inc. v. Schlack*, 71 F. Supp. 2d 299 (S.D.N.Y. 1999)).

<sup>51</sup> 114 P.L. 153, 130 Stat. at 384-385.

<sup>52</sup> *Id.*

<sup>53</sup> *Id.* at 385.

<sup>54</sup> *Id.*

## V. Conclusion

By adding a private civil claim for theft of trade secrets, federal law now provides protection to trade secrets in a manner similar to other forms of intellectual property (such as trademarks, copyrights and patents). While the full impact of DTSA will not be fully known until after a body of federal case law is developed construing its many significant provisions, it is clear, even at this early stage, that the statute will provide litigants and practitioners in New York new and stronger protections and remedies not available under the common law or even the proposed UTSA legislation.

Although DTSA seeks to create uniformity in trade secret law across state lines, the failure of DTSA to preempt state law dilutes the effectiveness of this stated purpose.<sup>55</sup> This may mean that it will take much longer for uniformity to develop until a substantial body of federal case law is established. Ultimately, however, it is expected that greater uniformity (and predictability for business decisions) will emerge, either through development of jurisprudence or by direct amendment.

New York litigators should take note of DTSA's rejection of the "inevitable disclosure doctrine" as a predicate to obtaining injunctive relief to prevent employment, which is a departure from both UTSA and New York law. Although the relatively weak state of this doctrine in New York may not represent a significant issue (particularly given the upside of the stronger remedial provisions found in DTSA), it is a factor that should be considered in deciding whether to proceed under DTSA or solely in state court under New York common law.<sup>56</sup> It should also be noted that the availability of the federal forum provides mechanisms under the Federal Rules of Civil Procedure which may be broader than what may exist in state court practice, including the availability of expert discovery.<sup>57</sup>

Finally, DTSA's whistleblower immunity notice requirements means that your clients may need to review and revise their non-disclosure, non-solicitation, and non-competition agreements to not only maximize the protections available under DTSA, but also ensure they are consistent with other changes in the ever-evolving case law on the subject. Moreover, there is also the possibility that the failure to include the immunity notice could be interpreted as evidence of overreaching for purposes of refusing to "blue pencil" or reform a restrictive covenant.<sup>58</sup>

---

<sup>55</sup> The lack of express preemption, means that New York litigators may still simultaneously assert both DTSA and common law theft of trade secret claims, which may also result in increased litigation costs.

<sup>56</sup> The statute of limitations under DTSA is three years, see 114 P.L. 153, 130 Stat. at 380, which is consistent with the limitations period for misappropriation of trade secrets in New York. See, CPLR § 214(4).

<sup>57</sup> Recent amendments to New York's Commercial Division Rules, however, are narrowing the gap between federal and state practice in cases subject to those rules. See, 22 N.Y.C.R.R. § 202.70.

<sup>58</sup> See, *Columbia Ribbon & Carbon Mfg. Co., Inc. v. A-1-A Corp.*, 42 N.Y.2d 496, 398 N.Y.S.2d 1004, 369 N.E.2d 4 (1977); *BDO Seidman v Hirshberg*, 93 NY2d 382, 388-389, 712 NE2d 1220, 690 NYS2d 854 (1999); *Brown & Brown, Inc. v. Johnson*, 115 A.D.3d 162, 980 N.Y.S.2d 631 (4th Dept. 2014).

## Head in the Cloud: The Insider Threat to a Company's Trade Secrets

By Bradley A. Hoppe and Heath J. Szymczak

Reprinted with permission from the April 4, 2016 edition of the New York Law Journal © 2016 ALM Media Properties, LLC. All rights reserved.  
Further duplication without permission is prohibited. ALMReprints.com - 877-257-3382 - reprints@alm.com.

After months of searching, a client finally hires its “dream candidate.” The client welcomes the new employee with open arms and wants to provide all the resources needed for the employee to succeed, entrusting the employee with access to its confidential information. Unbeknownst to the client, however, the new employee merely views the position as a stepping stone to something bigger. From day one on the job, he continues his job search, secretly reaching out to some of your client's biggest competitors (who also view him as a “dream candidate” partly because of his position with your client). A few months later, the honeymoon comes to an abrupt end when the employee puts in his notice that he is leaving for a new position with a competitor. The real shock is yet to come: when your client learns that its trusted employee has uploaded some of its most highly confidential competitive information (e.g., customer lists, pricing information, customer requirements, diagrams, specifications, manufacturing processes and formulae) to a thumb drive, personal email or, even worse, the cloud.

This nightmare hypothetical is all too common across all industries, yet many companies remain woefully unprepared. Perhaps as the result of the exposure by the media to the cybersecurity threats posed by outsiders, companies often overlook (and, in many cases, completely ignore) the more immediate and substantial threats posed by insiders, namely their own employees. Recent surveys of companies and their employees and analyses of trade secret cases in federal and state courts reveal the following startling facts: (1) trade secret thefts are on the rise, with the number of cases involving trade secret theft doubling between the years 1988 and 1995, doubling again between the years 1995 to 2004, and, at the current rate, likely doubling again by the year 2017;<sup>1</sup> (2) more than 85% of all trade secret thefts are believed to be perpetrated by an employee or business partner;<sup>2</sup> and (3) more than half of employees recently surveyed have admitted to taking information from their former employer and approximately 40% of those same employees acknowledged that they intended to use that information on behalf of their new employer.<sup>3</sup>

Despite these statistics and the significant threat posed by employee insiders, companies continue to grant employees nearly unfettered access to their trade secret information without any – let alone adequate – safeguards in place, often with disastrous and irreparable consequences to their business. This article will provide not only a general overview of the law of trade secrets, but also practical steps clients can take to better protect their information from the insider threat, as well as illustrative case examples of the consequences of failing to act.

### What Is a Trade Secret?

Unlike most other states, New York has not adopted any form of the Uniform Trade Secret Act, but instead relies on the following common law standard, as set forth in the Restatement of Torts § 757, comment b:

A trade secret is any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it. In deciding a trade secret claim several factors should be considered: (1) the extent to which the information is known outside of the business; (2) the extent to which it is known by employees and others involved in the business; (3) the extent of measures taken by the business to guard the secrecy of the information; (4) the value of the information

1 David S. Almeling, *Tracking Trade Secret Stats* (2010).

2 David S. Almeling, Darin W. Snyder, Michael Sapoznikow, Whitney E. McCollum and Jill Weader, *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 *Gonzaga Law Review* 291, 303 (2010).

3 Symantec Corporation, *What's Yours is Mine: How Employees are Putting Your Intellectual Property at Risk*, at 1 (2013).



to the business and its competitors; (5) the amount of effort or money expended by the business in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.<sup>4</sup>

Simply put, a trade secret can be anything which gives a company a competitive advantage and, most importantly, is kept secret and confidential. Trade secret information can take many forms and, so long as it meets the above standard, can include product designs, formulae, manufacturing processes, financial data, customer lists, customer requirements and pricing, source code, market research, and business plans.

### What Is the Biggest Threat to a Client's Trade Secrets?

Notwithstanding the time and resources clients often expend in developing valuable trade secret information, they remain vulnerable to the insider threat posed by their own employees.

It used to be that companies had to worry principally about the theft of physical files; this of course evolved as technology changed from the use of floppy disks, to CD's and DVD's, to the use of personal email accounts, to small USB based thumb drives to download and abscond with sensitive electronic files. Today, while some of these – thumb drives and personal email specifically – continue to be used by employees and present threats to our clients, they are far easier to prevent and detect than the potentially catastrophic threat posed by cloud computing generally and cloud-based storage specifically. These “USBs in the sky” allow an employee, who has access to commercially sensitive information and a personal cloud storage account through Dropbox, OneDrive, Google Drive, iCloud, etc., to upload trade secret and other confidential files to the “cloud.”<sup>5</sup> Once on the cloud, an employee can and often times does access, download and transfer to third parties his/her employer's trade secret and other commercially sensitive information. Not only can this cause significant and potentially irreparable harm to a client if the information falls into the hands of a competitor, but the fact that it can be disclosed to third parties and, in essence, made public, could very well deprive the client of the ability to obtain trade secret protection of that information down the road.

We are just now starting to see published cases coming out in state and federal courts involving the use of cloud computing for the purpose of misappropriating trade secret information. For example, in a case out of the Eastern District of Texas,<sup>6</sup> the defendant, plaintiff's former COO, utilized Dropbox on the day of her resignation to upload literally thousands of confidential patient files and other commercially sensitive trade secret files. Fortunately for that plaintiff, its former COO made an off-the-cuff comment to one of the plaintiff's human resource employees that “she knew where too many bodies were buried”, which led the employer to conduct a detailed forensic investigation of the former COO's computer equipment. Had no such comment been made and no investigation conducted revealing the use of Dropbox, there is no telling the amount of damage that could have been done to this plaintiff's business.

Similarly, in a case out of the Eastern District of Michigan,<sup>7</sup> an employer came to learn that one of its former employees, at or around the time of his resignation, uploaded myriad commercially sensitive files to Dropbox. The plaintiff there immediately brought an application for a preliminary injunction seeking to prevent that former employee from not only using the information taken, but also continuing to operate his competing business. While the court granted the injunction with respect to the use of the information and required that the information be returned and his computer, other electronic devices and cloud and other storage applications scrubbed *at plaintiff's cost*, the court refused to enjoin operations of the competing business due to the absence of a non-competition agreement or strong evidence that the commercially sensitive information was actually accessed and used post-resignation. Not only does this case illustrate the need for companies to implement policies designed to detect the use of cloud-based storage applications, but also for the use of reasonable restrictive covenants (e.g., non-disclosure and/or non-competition covenants) with strong attorneys' fees and cost shifting provisions.

4 *Ashland Management v. Janien*, 82 N.Y.2d 395, 407 (1993) (quoting Restatement of Torts § 757, comment b).

5 For those unfamiliar with the term, the “cloud” is best described as the use of a network of remote servers hosted on the internet to store, manage and process data, as opposed to the use of a local server or a personal computer.

6 *Frisco Medical Center, L.P. v. Bledsoe*, 2015 U.S. Dist. LEXIS 159915 (E.D. Tx. 2015).

7 *PrimePay, LLC v. Barnes*, 2015 U.S. Dist LEXIS 65710 (E.D. Mich. 2015).

With new technologies being developed every day, it is imperative to advise clients regarding the risks presented by employees generally and the use of cloud-based storage and other means to abscond with information, as well as the steps that can and should be taken to help lessen the risk of theft and, in the event that an employee succeeds, detect any such theft in a timely manner.

### **How Can Clients Protect their Trade Secrets From the Insider Threat?**

One of the best – and most common – ways to protect trade secret information, as well as the customer relationships and goodwill that an employer spends significant time and resources in developing, is through the use of reasonable restrictive covenants, such as non-disclosure, non-competition and/or non-solicitation provisions. Not only are restrictive covenants effective in preventing trade secret theft, but courts have made clear that where an employer fails to use such covenants, that employer cannot establish that it took reasonable steps to protect its information and thus have it recognized as “trade secrets” when forced to protect its rights in court.<sup>8</sup>

Where clients often get into trouble is that they try to restrict too much or use a “one size fits all” approach, both of which may subject the covenant to invalidation as overbroad or unnecessary to support a legitimate business purpose.<sup>9</sup> If used correctly and tailored to the particular employee and interest at stake (here, the protection against use and disclosure of trade secret information), a non-competition or other restrictive covenant can be one of the more effective tools in protecting against the theft or unauthorized use or disclosure of trade secret information, particularly when coupled with the additional deterrents of attorneys’ fee and forensic cost shifting provisions. It must be noted, however, that courts everywhere – including New York – are increasingly suspicious of restrictive covenants as a condition of employment, either initial or continued; it is thus imperative that a client consult with counsel to draft and/or review their restrictive covenants prior to presenting them to their employees, particularly with the recent trend to invalidate entire covenants if there exists evidence of overreaching and/or coercion.<sup>10</sup>

In addition to the use of reasonable restrictive covenants tailored to the specific employee with access to trade secret information, clients must implement policies designed to protect their valuable information. Many clients, however, continue to grant certain of their employees, even those with no legitimate business reason, nearly unfettered access to what they consider to be their trade secret information. It is imperative for a client hoping to obtain trade secret protection from the courts to implement some combination of the following common sense policies:

- *Limit access to trade secret information* to only those employees who need it to perform their job responsibilities. Not only does this limit the universe of potential threats, but it also shows a court that reasonable steps were taken to protect information in the event that a theft occurs and protection is needed.
- *Implement policies to address the use of cloud storage.* With respect to personal cloud-based storage, it is recommended that clients not only prohibit the use of such storage applications, but work with their internal IT departments to disable the ability of employees to utilize them. In addition, where a client utilizes employer-based cloud storage, the client must ensure that proper safeguards are being used to monitor and track access, such as unique log-in credentials for each employee.
- *Conspicuously designate confidential or trade secret documents* so that employees are on clear notice as to how they should handle certain materials.

<sup>8</sup> See, *Delta Filter Corp. v. Morin*, 108 A.D.2d 991(3d Dept 1985) (holding that in the absence of a nondisclosure agreement the plaintiff could not establish that the defendant used improper or wrongful means to obtain plaintiff’s purported trade secret information); see also, *Starlight Limousine Serv. v. Cucinella*, 275 A.D.2d 704 (2d Dept. 2000) (holding that information did not constitute trade secrets where the company failed to require the employee to execute any kind of agreement to keep the information secret or not use the information after leaving employment).

<sup>9</sup> See, e.g., *Bdo Seidman v. Hirshberg*, 93 N.Y.2d 382 (1999).

<sup>10</sup> *Bdo Seidman v. Hirshberg*, 93 N.Y.2d 382 (1999); *Scott, Stackrow & Co., C.P.A’s, P.C. v. Skavina*, 9 A.D.3d 805 (3d Dept. 2004); *Gilman & Ciocia, Inc. v. Randello*, 55 A.D.3d 871 (2d Dept. 2008); *Brown & Brown, Inc. v. Johnson*, 115 A.D.3d 162 (4th Dept. 2014), *reversed on other grounds*, 25 N.Y.3d 364 (2015).

- *Implement policies to monitor and track* an employee's access to and use of trade secret information.
- *Prepare written trade secret protection policies for access to and use of company information.* Such policies should, at the very least, be distributed to, and reviewed and initialed by, any employee with access to trade secrets.
- *Exit interviews.* All clients should conduct an exit interview of all departing employees and, as a part of each such interview, remind that employee in writing of his/her contractual and common law obligations with respect to company information, post-employment obligations and prohibitions, etc.
- *Collect and secure computers and electronic devices used by terminated employees.* Computers and electronic devices need to be set aside in a secure place and, without exception, not placed back into circulation unless such computers and devices have already been imaged by a forensic consultant.

Lastly, given the significant risks posed by employees to a client's trade secret information and other intangible assets, it is advisable for clients to routinely have their policies and procedures, as well as their restrictive covenants, audited and updated to better ensure that they are in compliance with the ever-changing law and best practices. As any trade secret litigator (or any business owner forced to litigate a trade secret in court) will surely attest, the nominal cost to a client associated with such a periodic preventative audit pales in comparison to the costs associated with either the loss of a trade secret or litigation to protect and enforce trade secret and other related rights. As the old saying goes, an ounce of prevention is worth a pound of cure.

*Bradley A. Hoppe and Heath J. Szymczak are Members of the Litigation Practice Group of Bond, Schoeneck & King PLLC. Mr. Hoppe has extensive experience in commercial and defense matters, including unfair competition and trade secret claims. Mr. Szymczak regularly counsels clients on trade secret theft prevention, particularly from former employees.*

*Messrs. Hoppe and Szymczak helped develop the innovative Bond Trade Secret Protection Audit which systematically reviews a company's agreements, policies and protocols, as well as their physical and electronic security measures.*



Commitment • Service • Value • Our Bond



Bond, Schoeneck & King PLLC (Bond, we, or us), has prepared this communication to present only general information. This is not intended as legal advice, nor should you consider it as such. You should not act, or decline to act, based upon the contents. While we try to make sure that the information is complete and accurate, laws can change quickly. You should always formally engage a lawyer of your choosing before taking actions which have legal consequences.

For information about our firm, practice areas and attorneys, visit our website, [www.bsk.com](http://www.bsk.com). • Attorney Advertising • © 2015 Bond, Schoeneck & King, PLLC

CONNECT WITH US ON LINKEDIN: SEARCH FOR BOND, SCHOENECK & KING, PLLC

FOLLOW US ON TWITTER: SEARCH FOR BONDLAWFIRM

## New Federal Law Means You Should Update Your Non-Compete And Non-Disclosure Agreements

President Obama this week (on May 11) signed into law the Defend Trade Secrets Act (DTSA) of 2016. This is truly a landmark law; one that expands the federal remedies companies can pursue to halt the theft of trade secrets vital to a company's operation and financial security. DTSA received unprecedented bipartisan support, with passage by 87-0 in the Senate, 410-2 in the House of Representatives.

This new law recognizes the vital role that trade secrets play in generating billions of dollars in annual revenues and millions of jobs as a key component of our national – and local – economy. It also comes in response to several high profile cases which demonstrate how vulnerable U.S. companies are from internal and external cyber-threats.

A trade secret is anything which gives a company a competitive advantage and is kept confidential, including a design, formula, manufacturing process, financial data, or customer information. Prior to DTSA, trade secrets did not receive the same protections afforded to other forms of intellectual property such as trademarks, copyrights, and patents.

DTSA provides the first ever federal civil statutory remedies for theft of trade secrets. These remedies exceed those which may have been previously available under state law, including aggressive ex parte seizure mechanisms similar to those used to seize counterfeit goods under trademark law, exemplary damages, and attorney fees.

There is a caveat: imbedded within the text of DTSA is a warning that if you fail to include whistleblower immunity notice in any agreement with an employee that governs the use of a trade secret or other confidential information you will not be able to take advantage of the exemplary damages and attorney fees available under DTSA.

This notice must inform the employee, among other things, that he or she cannot be held liable under any trade secret law for the disclosure of a trade secret that is made (1) in confidence to a government official or to an attorney for the sole purpose of reporting a suspected violation of law or (2) in a document in a lawsuit or proceeding filed under seal.

Non-compete and non-disclosure agreements play a key role in protecting a company's trade secrets. The law governing the enforceability of these agreements is constantly changing. Failure to revise these agreements periodically could have disastrous consequences. The passage of DTSA provides yet another reason why you need to review and revise your agreements to maximize the protections available. A simple and cost effective way to have your agreements reviewed, along with your physical and digital security measures, is through Bond Schoeneck & King's innovative [Trade Secret Protection Audit](#).

To learn more, contact [Bradley A. Hoppe](#) (716.416.7025; [bhoppe@bsk.com](mailto:bhoppe@bsk.com)) or [Heath J. Szymczak](#) (716.416.7057; [hszymczak@bsk.com](mailto:hszymczak@bsk.com)).



Commitment • Service • Value • Our Bond



Bond, Schoeneck & King PLLC (Bond, we, or us), has prepared this communication to present only general information. This is not intended as legal advice, nor should you consider it as such. You should not act, or decline to act, based upon the contents. While we try to make sure that the information is complete and accurate, laws can change quickly. You should always formally engage a lawyer of your choosing before taking actions which have legal consequences.

For information about our firm, practice areas and attorneys, visit our website, [www.bsk.com](http://www.bsk.com). • Attorney Advertising • © 2016 Bond, Schoeneck & King, PLLC

CONNECT WITH US ON LINKEDIN: SEARCH FOR BOND, SCHOENECK & KING, PLLC

FOLLOW US ON TWITTER: SEARCH FOR BONDLAWFIRM

Restatement (First) of Torts § 757 (1939)

Restatement of the Law - Torts

Database updated June 2014  
Restatement (First) of Torts

Division 9. Interference with Business Relations

Part 1. By Trade Practices

Chapter 36. Miscellaneous Trade Practices

§ 757 Liability for Disclosure or Use of Another's Trade Secret—General Principle

Comment:

Case Citations - by Jurisdiction

**One who discloses or uses another's trade secret, without a privilege to do so, is liable to the other if**

- (a) he discovered the secret by improper means, or**
- (b) his disclosure or use constitutes a breach of confidence reposed in him by the other in disclosing the secret to him, or**
- (c) he learned the secret from a third person with notice of the facts that it was a secret and that the third person discovered it by improper means or that the third person's disclosure of it was otherwise a breach of his duty to the other, or**
- (d) he learned the secret with notice of the facts that it was a secret and that its disclosure was made to him by mistake.**

---

***Comment:***

*a. Rationale.* The privilege to compete with others (see § 708, vol. III) includes a privilege to adopt their business methods, ideas or processes of manufacture. Were it otherwise, the first person in the field with a new process or idea would have a monopoly which would tend to prevent competition. This privilege has some limitations, however. In the first place, in order to promote the progress of science and the useful arts, patent and copyright laws provide protection to the originator. The patent laws prohibit the witting or unwitting manufacture, sale or use by any person of a device, process or article which infringes a patent granted to another. The copyright laws prohibit the plagiarism of a work copyrighted by another. The protection afforded by both types of legislation is limited to a fixed number of years. Both types of legislation establish a monopoly for the purpose of encouraging invention and art. In the second place, the law of torts prohibits copying in a manner which creates in the market avoidable confusion of commercial source. The privilege to copy is not a privilege to palm off one's goods as those of another. Thus, when the physical appearance of one's goods has acquired in the market a significance as identifying the goods of which he is the commercial source, another may not copy that appearance if it is non-functional, and if it is functional, he may copy it only upon taking reasonable precaution to avoid confusion (see § 741, vol. III). The rule stated in this Section is a further limitation on the privilege to copy when the thing copied is a trade secret. This limitation is not imposed because of any difference in function or value between trade secrets and other devices or processes. A formula for a medicinal compound or a process of manufacture is equally effective in making its product when the formula or process is generally known as when it is secret. Its original discovery may require equal ingenuity and labor when it must necessarily be disclosed by the product which results from it as when it can be kept secret. Exclusion of others from the privilege of using it will give it the same value to the originator in the one case as in the other. Indeed, a patent

monopoly is granted only upon full disclosure of the subject matter of the patent. The significant difference of fact between trade secrets and processes or devices which are not secret is that knowledge of the latter is available to the copier without the use of improper means to procure it, while knowledge of the former is ordinarily available to him only by the use of such means. It is the employment of improper means to procure the trade secret, rather than the mere copying or use, which is the basis of the liability under the rule stated in this Section.

There is considerable discussion in judicial opinions as to the basis of liability for the disclosure or use of another's trade secrets. Analogy is sometimes found in the law of "literary property," copyright, patents, trade-marks and unfair competition. The suggestion that one has a right to exclude others from the use of his trade secret because he has a right of property in the idea has been frequently advanced and rejected. The theory that has prevailed is that the protection is afforded only by a general duty of good faith and that the liability rests upon breach of this duty; that is, breach of contract, abuse of confidence or impropriety in the method of ascertaining the secret. Apart from breach of contract, abuse of confidence or impropriety in the means of procurement, trade secrets may be copied as freely as devices or processes which are not secret. One who discovers another's trade secret properly, as, for example; by inspection or analysis of the commercial product embodying the secret, or by independent invention, or by gift or purchase from the owner, is free to disclose it or use it in his own business without liability to the owner. As to the liability of one who procures the secret from a third person without notice of any impropriety in the third person's disclosure of it, see § 758. As to the procurement of information other than trade secrets, see § 759. For a definition of trade secrets, see Comment *b*.

The protection afforded by the rule stated in this Section is in some respects greater and in some respects less than that afforded by the patent law. It is greater in that it is not limited to a fixed number of years and does not require novelty and invention as in the case of patents (see Comment *b*). It is less in that secrecy of the process and impropriety in the method of procuring the secret are requisite here but not in the case of patents.

*b. Definition of trade secret.* A trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it. It may be a formula for a chemical compound, a process of manufacturing, treating or preserving materials, a pattern for a machine or other device, or a list of customers. It differs from other secret information in a business (see § 759) in that it is not simply information as to single or ephemeral events in the conduct of the business, as, for example, the amount or other terms of a secret bid for a contract or the salary of certain employees, or the security investments made or contemplated, or the date fixed for the announcement of a new policy or for bringing out a new model or the like. A trade secret is a process or device for continuous use in the operation of the business. Generally it relates to the production of goods, as, for example, a machine or formula for the production of an article. It may, however, relate to the sale of goods or to other operations in the business, such as a code for determining discounts, rebates or other concessions in a price list or catalogue, or a list of specialized customers, or a method of bookkeeping or other office management.

*Secrecy.* The subject matter of a trade secret must be secret. Matters of public knowledge or of general knowledge in an industry cannot be appropriated by one as his secret. Matters which are completely disclosed by the goods which one markets cannot be his secret. Substantially, a trade secret is known only in the particular business in which it is used. It is not requisite that only the proprietor of the business know it. He may, without losing his protection, communicate it to employees involved in its use. He may likewise communicate it to others pledged to secrecy. Others may also know of it independently, as, for example, when they have discovered the process or formula by independent invention and are keeping it secret. Nevertheless, a substantial element of secrecy must exist, so that, except by the use of improper means, there would be difficulty in acquiring the information. An exact definition of a trade secret is not possible. Some factors to be considered in determining whether given information is one's trade secret are: (1) the extent to which the information is known outside of his business; (2) the extent to which it is known by employees and others involved in his business; (3) the extent of measures taken by him to guard the secrecy of the information; (4) the value of the information to him and to his competitors; (5) the amount of effort or money expended by him in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.

*Novelty and prior art.* A trade secret may be a device or process which is patentable; but it need not be that. It may be a device or process which is clearly anticipated in the prior art or one which is merely a mechanical improvement that a good mechanic can make. Novelty and invention are not requisite for a trade secret as they are for patentability. These requirements are essential to patentability because a patent protects against unlicensed use of the patented device or process



even by one who discovers it properly through independent research. The patent monopoly is a reward to the inventor. But such is not the case with a trade secret. Its protection is not based on a policy of rewarding or otherwise encouraging the development of secret processes or devices. The protection is merely against breach of faith and reprehensible means of learning another's secret. For this limited protection it is not appropriate to require also the kind of novelty and invention which is a requisite of patentability. The nature of the secret is, however, an important factor in determining the kind of relief that is appropriate against one who is subject to liability under the rule stated in this Section. Thus, if the secret consists of a device or process which is a novel invention, one who acquires the secret wrongfully is ordinarily enjoined from further use of it and is required to account for the profits derived from his past use. If, on the other hand, the secret consists of mechanical improvements that a good mechanic can make without resort to the secret, the wrongdoer's liability may be limited to damages, and an injunction against future use of the improvements made with the aid of the secret may be inappropriate.

*Information not a trade secret.* Although given information is not a trade secret, one who receives the information in a confidential relation or discovers it by improper means may be under some duty not to disclose or use that information. Because of the confidential relation or the impropriety of the means of discovery, he may be compelled to go to other sources for the information. As stated in Comment *a*, even the rule stated in this Section rests not upon a view of trade secrets as physical objects of property but rather upon abuse of confidence or impropriety in learning the secret. Such abuse or impropriety may exist also where the information is not a trade secret and may be equally a basis for liability. The rules relating to the liability for duties arising from confidential relationships generally are not within the scope of the Restatement of this Subject. As to the use of improper means to acquire information, see § 759.

*c. Disclosure or use.* One who has a trade secret may be harmed merely by the disclosure of his secret to others as well as by the use of his secret in competition with him. A mere disclosure enhances the possibilities of adverse use. The persons to whom the disclosure is made may or may not be liable under Clause (c) for the subsequent use (see also § 758). Since a trade secret is vendible and since its sale value depends in part upon its secrecy, a mere disclosure may reduce the vendibility or sale value of the secret. The rule stated in this Section protects the interest in a trade secret against both disclosure and adverse use.

The duties not to disclose and not to use another's trade secret are not, however, necessarily concomitant, though they are frequently found together. Thus, a former employee to whom the secret was communicated in the course of his employment may be under both duties (see Restatement of Agency, §§ 395 and 396). On the other hand, a manufacturer who is permitted by the owner of the secret to use it in his manufacturing may be subject only to a duty not to disclose the secret to third persons. Or the manufacturer may be permitted to use the secret only in the manufacture of products for the owner, with a duty not to disclose the secret or use it in the manufacture of products on his own account or for others.

*Modification or improvement of the secret by the actor.* To subject a person to liability, under the rule stated in this Section, for the use of another's trade secret, there is no requirement that he use it in exactly the form in which he received it. He may be liable even if he uses it with modifications or improvements upon it effected by his own efforts. Differences in detail do not preclude liability if, substantially, the process used by the actor is derived from the other's secret in the manner stated in this Section. The liability is avoided only when the contribution by the other's secret is so slight that the actor's process can be said to be derived from other sources; although even in such a case the actor is still subject to liability for harm caused by his disclosure or possession of the secret, under the rules stated in §§ 757- 759. The extent of the modifications or improvements made by the actor upon the other's secret may, however, affect the computation of damages or profits for which he is liable to the other.

*d. Privilege.* A privilege to disclose or use another's trade secret may arise from the other's consent or from other conduct on his part by which he is estopped from complaining. A privilege to disclose may also be given by the law, independently of the other's consent, in order to promote some public interest. Thus, a witness who is compelled by law to answer a question which calls for a disclosure of the secret is not liable for making the disclosure in his answer. Or the privilege may be given to protect an interest of the actor, as, for example, when disclosure may be necessary to defend a charge of infringement. In order to protect trade secrets against disclosure in the course of litigation, testimony involving such disclosure is generally taken by the court privately rather than in public and the record of such testimony is appropriately safeguarded against public disclosure.

*e. Remedies.* One who has a right under the rule stated in this Section is entitled to a remedy or remedies appropriate under the circumstances. He may recover damages for past harm, or be granted an injunction against future harm by disclosure or adverse use, or be granted an accounting of the wrongdoer's profits, or have the physical things embodying the secret, such as designs, patterns and so forth, surrendered by the wrongdoer for destruction. Moreover, he may have two or more of these remedies in the same action if the court is competent to administer them. Defenses generally available in tort actions and actions for injunctive relief are also available here, insofar as they are applicable,

---

**Comment on Clause (a):**

*f. Improper means of discovery.* The discovery of another's trade secret by improper means subjects the actor to liability independently of the harm to the interest in the secret. Thus, if one uses physical force to take a secret formula from another's pocket, or breaks into another's office to steal the formula, his conduct is wrongful and subjects him to liability apart from the rule stated in this Section. Such conduct is also an improper means of procuring the secret under this rule. But means may be improper under this rule even though they do not cause any other harm than that to the interest in the trade secret. Examples of such means are fraudulent misrepresentations to induce disclosure, tapping of telephone wires, eavesdropping or other espionage. A complete catalogue of improper means is not possible. In general they are means which fall below the generally accepted standards of commercial morality and reasonable conduct. See also, § 759, Comment *c*.

*g. Actor's purpose.* Liability under the rule stated in this Section is based not on the actor's purpose to discover another's trade secret but on the nature of the conduct by which the discovery is made. The actor is free to engage in any proper conduct for the very purpose of discovering the secret. So long as his conduct is proper, his purpose does not subject him to liability. Conversely, if his conduct is improper, he is subject to liability even though he engaged in the conduct for a purpose other than that of discovering the trade secret.

*Illustrations:*

**Illustrations:**

1. A wishes to recover from B amorous letters sent to B by A's wife. Learning that the letters are in a safe in B's office, he breaks into the safe at night and removes a bundle of papers which he believes to be the desired letters. When he examines the bundle at his own office, he finds that it contains the secret formulas for the compounds which B markets. Fearing that a return of the papers might disclose his crime, he keeps them. Three months later he begins to manufacture compounds on the basis of the stolen formulas. A is liable to B under the rule stated in this Section.
2. A manufactures and sells a medicinal compound from a formula which is his trade secret. B wishes to manufacture and sell the same compound. He engages competent technicians to discover the formula. By scientific analysis of and experimentation with A's compound, the technicians do discover the formula. B then begins to manufacture and sell a compound made in accordance with the formula. B is not liable to A under the rule stated in this Section.

*h. Improper means employed against third person.* The rule stated in Clause (a) of this Section applies to improper means in procuring the secret not only from the owner but also from any third person holding the secret under a duty to the owner not to disclose it to others. Thus, the rule applies to a theft of the secret from an employee of the owner or from a post office or a bank, or from any other person to whom the secret was entrusted in confidence. If the actor procures the secret by a voluntary disclosure by such third person in breach of his duty and the actor employs no improper means to cause the disclosure, he is not subject to liability under the rule stated in Clause (a), though he may be liable under the rule stated in Clause (c). But if the actor intentionally procures the third person to make a disclosure in breach of his duty, the actor may be liable under both rules; under the former because inducing one to commit a breach of duty is an improper means of procuring the secret; and under the latter because of the actor's knowledge of the breach.

*i. Procuring third person to employ improper means.* The rule stated in Clause (a) applies to the case in which the actor procures a third person to discover the secret by improper means, as when A hires B to steal a trade secret from C's safe. If,



however, A does not authorize the use of improper means, he is subject to liability only under the rule stated in Clause (c).

---

*Comment on Clause (b):*

*j. Breach of confidence.* A breach of confidence under the rule stated in this Clause may also be a breach of contract which subjects the actor to liability under the rules stated in the Restatement of Contracts. But whether or not there is a breach of contract, the rule stated in this Section subjects the actor to liability if his disclosure or use of another's trade secret is a breach of the confidence reposed in him by the other in disclosing the secret to him. The chief example of a confidential relationship under this rule is the relationship of principal and agent (see Restatement of Agency, §§ 395 and 396). Such is also the relationship between partners or other joint adventurers. But this confidence may exist also in other situations. For example, A has a trade secret which he wishes to sell with or without his business. B is a prospective purchaser. In the course of negotiations, A discloses the secret to B solely for the purpose of enabling him to appraise its value. Or, A requests a loan from B, a banker, for the purpose of aiding the manufacture of a product by A's secret process. In order to assure B about the soundness of the loan, A discloses the secret to him in confidence. In both cases B is under a duty not to disclose the secret or use it adversely to A. Again, this confidence may exist even when no business relation between A and B exists or is contemplated, as when A comes to B, his former teacher, for free advice which B is willing to give with respect to the secret and discloses the secret to him in confidence. But in all these cases A cannot impose a confidence on B without B's consent. If A discloses the secret to B despite B's protest that he does not wish to hold it in confidence and will not so hold it if it is disclosed, the confidence requisite for liability under the rule stated in Clause (b) does not arise. Likewise, the confidence does not arise if B has no notice of the confidential character of the disclosure. But no particular form of notice is required. The question is simply whether in the circumstances B knows or should know that the information is A's trade secret and that its disclosure is made in confidence. As to disclosure by mistake see Comment *o*.

---

*Comment on Clause (c):*

*k. Limitations of Clause (c).* This Clause applies only to the cases in which the actor has the stated notice when he first learns the secret. For the rules relating to cases in which he acquires the notice after he learned the secret, see § 758. Again, Clause (c) deals primarily with the situations in which the actor does not knowingly procure the third person to use improper means or to violate his duty otherwise. But such cases are not excluded from this Clause, and the rules stated in both this Clause and Clause (a) may be applicable to them.

*l. What is notice.* One has notice of facts under the rule stated in this Section when he knows of them or when he should know of them (see Restatement of Trusts, § 297). He should know of them if, from the information which he has, a reasonable man would infer the facts in question, or if, under the circumstances, a reasonable man would be put on inquiry and an inquiry pursued with reasonable intelligence and diligence would disclose the facts. One may have notice of a fact because he has been given a notification of it. Under the rule stated in the Restatement of Agency, § 9, a person is given notification of a fact by another if the latter (a) informs him of the fact or of other facts from which he has reason to know or should know the fact, or (b) does an act which, under the rules applicable to the transaction, has the same effect on the legal relations of the parties as the acquisition of knowledge. Notification by the second method includes, for example, recordation, which is generally not applicable to the situations dealt with in this Section, and delivery of a letter to a person's office where it is subsequently lost without having been read by him (see Restatement of Agency, § 9, Comments *e-g* and § 11).

*Illustrations:*

**Illustrations:**

3. A and B are competitors. A knows that B has a secret process for treating his goods which reduces his manufacturing costs by 7 per cent. C comes to A and offers to sell him B's secret. A does not know C and does not

know how C discovered the secret. On these facts a finding that A has notice that C's disclosure is in breach of his duty is proper.

4. A and B are competitors. C is, to A's knowledge, a trusted employee of B. C comes to A and offers to sell him a process for treating his goods. A does not know that the process is B's trade secret but he does know that there are several trade secrets employed by his competitors and that the process offered by C is novel to A and is valuable for the businesses of both A and B. On these facts a finding that A has notice that the process is B's trade secret and that C is disclosing it in breach of duty is proper.

*m. Notice of secrecy and of breach of duty.* The actor is subject to liability under the rule stated in this Clause only if he has notice of both the fact that the information is secret and the fact that the disclosure by the third person is a breach of his duty. But frequently the two facts are mutually dependent and notice of the one is also notice of the other. Thus, if the actor knows that the information proffered to him by one person is the trade secret of another he is put on inquiry as to the former's authority to disclose the information (see Comment l, Illustrations 3 and 4).

*n. Third person's breach of duty.* The breach of duty by the third person under the rule stated in this Clause is a breach which subjects him to liability for disclosing the trade secret. His duty not to disclose may arise out of a contract made by him or it may be based on the rules stated in Clauses (a), (b) and (d) of this Section.

*Illustrations:*

**Illustrations:**

5. A, who knows B's trade secret, makes a contract with B not to disclose it. Later A discloses the secret to C, who knows or should know of the contract. If C subsequently discloses or uses the secret, he is subject to liability to B under the rule stated in Clause (c).
6. A steals B's trade secret from B's safe and sells the secret to C, who has notice of the facts. If C subsequently discloses or uses the secret, he is subject to liability to B under the rule stated in Clause (c).
7. B communicates his trade secret to A in confidence under such circumstances that A is under a duty not to disclose or use the secret. A subsequently discloses the secret to C, who has notice of the facts. C later discloses or uses the secret. C is subject to liability to B under the rule stated in Clause (c).
8. A learns B's trade secret by reading a letter mistakenly delivered to him. A knows of the mistake and realizes that the information is B's trade secret. Later A discloses the secret to C, who has notice of the facts. C then discloses or uses the secret. C is subject to liability to B under the rule stated in Clause (c).

---

**Comment on Clause (d):**

*o. Knowledge of secret acquired by mistake.* In the situations covered by Clause (d), the actor need not be guilty of improper conduct in discovering the secret. If he makes the mistake, as, for example, in opening a letter not addressed to him, his mistake may be innocent or careless. Or the mistake may be made by another person, as, for example, in addressing the letter to him when someone else is intended. However the mistake is committed, if the actor has notice that the information is disclosed to him by mistake and that it is another's trade secret, good faith requires that he do not take advantage of the mistake and he is under a duty not to disclose or use the secret.

---

**Case Citations - by Jurisdiction**

U.S.

[Congress](#) (/congress) / [Bills](#) (/congress/bills) / [S. 1890 \(114th\)](#) (/congress/bills/114/s1890) / [Text](#)

## S. 1890: Defend Trade Secrets Act of 2016

[Overview](#) (/congress/bills/114/s1890) [Summary](#) (/congress/bills/114/s1890/summary) [Details](#) (/congress/bills/114/s1890/details) [Text](#) (/congress/bills/114/s1890/text)

The text of the bill below is as of **Apr 29, 2016** (Passed Congress/Enrolled Bill).

[Download PDF \(https://www.gpo.gov/fdsys/pkg/BILLS-114s1890enr/pdf/BILLS-114s1890enr.pdf\)](https://www.gpo.gov/fdsys/pkg/BILLS-114s1890enr/pdf/BILLS-114s1890enr.pdf)

[View Options](#)

Source: [GPO \(http://www.gpo.gov/fdsys/search/pagedetails.action?packageId=BILLS-114s1890enr\)](http://www.gpo.gov/fdsys/search/pagedetails.action?packageId=BILLS-114s1890enr)

ONE HUNDRED FOURTEENTH CONGRESS OF THE UNITED STATES OF AMERICA

2D SESSION

Begun and held at the City of Washington on Monday, the fourth day of January, two thousand and sixteen

### S. 1890

#### AN ACT

To amend chapter 90 of title 18, United States Code, to provide Federal jurisdiction for the theft of trade secrets, and for other purposes.

#### Section 1. Short title

This Act may be cited as the "Defend Trade Secrets Act of 2016".

#### Sec. 2. Federal jurisdiction for theft of trade secrets

(a) In general.—

Section 1836 of title 18, United States Code, is amended by striking subsection (b) and inserting the following:

(b) Private civil actions.—

(1) In general.—

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.

(2) Civil seizure.—

(A) In general.—

(i) Application.—

Based on an affidavit or verified complaint satisfying the requirements of this paragraph, the court may, upon ex parte application but only in extraordinary circumstances, issue an order providing for the seizure of property necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action.

(ii) Requirements for issuing order.—

The court may not grant an application under clause (i) unless the court finds that it clearly appears from specific facts that—

(I) an order issued pursuant to Rule 65 of the Federal Rules of Civil Procedure or another form of equitable relief would be inadequate to achieve the purpose of this paragraph because the party to which the order would be issued would evade, avoid, or otherwise not comply with such an order;

(II) an immediate and irreparable injury will occur if such seizure is not ordered;

(III) the harm to the applicant of denying the application outweighs the harm to the legitimate interests of the person against whom seizure would be ordered of granting the application and substantially outweighs the harm to any third parties who may be harmed by such seizure;

(IV) the applicant is likely to succeed in showing that—

- (aa) the information is a trade secret; and
  - (bb) the person against whom seizure would be ordered—
    - (AA) misappropriated the trade secret of the applicant by improper means; or
    - (BB) conspired to use improper means to misappropriate the trade secret of the applicant;
  - (V) the person against whom seizure would be ordered has actual possession of—
    - (aa) the trade secret; and
    - (bb) any property to be seized;
  - (VI) the application describes with reasonable particularity the matter to be seized and, to the extent reasonable under the circumstances, identifies the location where the matter is to be seized;
  - (VII) the person against whom seizure would be ordered, or persons acting in concert with such person, would destroy, move, hide, or otherwise make such matter inaccessible to the court, if the applicant were to proceed on notice to such person; and
  - (VIII) the applicant has not publicized the requested seizure.
- (B) Elements of order.—
- If an order is issued under subparagraph (A), it shall—
- (i) set forth findings of fact and conclusions of law required for the order;
  - (ii) provide for the narrowest seizure of property necessary to achieve the purpose of this paragraph and direct that the seizure be conducted in a manner that minimizes any interruption of the business operations of third parties and, to the extent possible, does not interrupt the legitimate business operations of the person accused of misappropriating the trade secret;
  - (iii)
    - (I) be accompanied by an order protecting the seized property from disclosure by prohibiting access by the applicant or the person against whom the order is directed, and prohibiting any copies, in whole or in part, of the seized property, to prevent undue damage to the party against whom the order has issued or others, until such parties have an opportunity to be heard in court; and
    - (II) provide that if access is granted by the court to the applicant or the person against whom the order is directed, the access shall be consistent with subparagraph (D);
  - (iv) provide guidance to the law enforcement officials executing the seizure that clearly delineates the scope of the authority of the officials, including—
    - (I) the hours during which the seizure may be executed; and
    - (II) whether force may be used to access locked areas;
  - (v) set a date for a hearing described in subparagraph (F) at the earliest possible time, and not later than 7 days after the order has issued, unless the party against whom the order is directed and others harmed by the order consent to another date for the hearing, except that a party against whom the order has issued or any person harmed by the order may move the court at any time to dissolve or modify the order after giving notice to the applicant who obtained the order; and
  - (vi) require the person obtaining the order to provide the security determined adequate by the court for the payment of the damages that any person may be entitled to recover as a result of a wrongful or excessive seizure or wrongful or excessive attempted seizure under this paragraph.
- (C) Protection from publicity.—
- The court shall take appropriate action to protect the person against whom an order under this paragraph is directed from publicity, by or at the behest of the person obtaining the order, about such order and any seizure under such order.
- (D) Materials in custody of court.—
- (i) In general.—
 

Any materials seized under this paragraph shall be taken into the custody of the court. The court shall secure the seized material from physical and electronic access during the seizure and while in the custody of the court.
  - (ii) Storage medium.—
 

If the seized material includes a storage medium, or if the seized material is stored on a storage medium, the court shall prohibit the medium from being connected to a network or the Internet without the consent of both parties, until the hearing required under subparagraph (B)(v) and described in subparagraph (F).

## (iii) Protection of confidentiality.—

The court shall take appropriate measures to protect the confidentiality of seized materials that are unrelated to the trade secret information ordered seized pursuant to this paragraph unless the person against whom the order is entered consents to disclosure of the material.

## (iv) Appointment of special master.—

The court may appoint a special master to locate and isolate all misappropriated trade secret information and to facilitate the return of unrelated property and data to the person from whom the property was seized. The special master appointed by the court shall agree to be bound by a non-disclosure agreement approved by the court.

## (E) Service of order.—

The court shall order that service of a copy of the order under this paragraph, and the submissions of the applicant to obtain the order, shall be made by a Federal law enforcement officer who, upon making service, shall carry out the seizure under the order. The court may allow State or local law enforcement officials to participate, but may not permit the applicant or any agent of the applicant to participate in the seizure. At the request of law enforcement officials, the court may allow a technical expert who is unaffiliated with the applicant and who is bound by a court-approved non-disclosure agreement to participate in the seizure if the court determines that the participation of the expert will aid the efficient execution of and minimize the burden of the seizure.

## (F) Seizure hearing.—

## (i) Date.—

A court that issues a seizure order shall hold a hearing on the date set by the court under subparagraph (B)(v).

## (ii) Burden of proof.—

At a hearing held under this subparagraph, the party who obtained the order under subparagraph (A) shall have the burden to prove the facts supporting the findings of fact and conclusions of law necessary to support the order. If the party fails to meet that burden, the seizure order shall be dissolved or modified appropriately.

## (iii) Dissolution or modification of order.—

A party against whom the order has been issued or any person harmed by the order may move the court at any time to dissolve or modify the order after giving notice to the party who obtained the order.

## (iv) Discovery time limits.—

The court may make such orders modifying the time limits for discovery under the Federal Rules of Civil Procedure as may be necessary to prevent the frustration of the purposes of a hearing under this subparagraph.

## (G) Action for damage caused by wrongful seizure.—

A person who suffers damage by reason of a wrongful or excessive seizure under this paragraph has a cause of action against the applicant for the order under which such seizure was made, and shall be entitled to the same relief as is provided under section 34(d)(11) of the Trademark Act of 1946 (15 U.S.C. 1116(d)(11)). The security posted with the court under subparagraph (B)(vi) shall not limit the recovery of third parties for damages.

## (H) Motion for encryption.—

A party or a person who claims to have an interest in the subject matter seized may make a motion at any time, which may be heard ex parte, to encrypt any material seized or to be seized under this paragraph that is stored on a storage medium. The motion shall include, when possible, the desired encryption method.

## (3) Remedies.—

In a civil action brought under this subsection with respect to the misappropriation of a trade secret, a court may—

## (A) grant an injunction—

(i) to prevent any actual or threatened misappropriation described in paragraph (1) on such terms as the court deems reasonable, provided the order does not—

(I) prevent a person from entering into an employment relationship, and that conditions placed on such employment shall be based on evidence of threatened misappropriation and not merely on the information the person knows; or

(II) otherwise conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business;

(ii) if determined appropriate by the court, requiring affirmative actions to be taken to protect the trade secret; and

(iii) in exceptional circumstances that render an injunction inequitable, that conditions future use of the trade secret upon payment of a reasonable royalty for no longer than the period of time for which such use could have been prohibited;

## (B) award—

## (i)

(I) damages for actual loss caused by the misappropriation of the trade secret; and

(II) damages for any unjust enrichment caused by the misappropriation of the trade secret that is not addressed in computing damages for actual loss; or

(ii) in lieu of damages measured by any other methods, the damages caused by the misappropriation measured by imposition of liability for a reasonable royalty for the misappropriator's unauthorized disclosure or use of the trade secret;

(C) if the trade secret is willfully and maliciously misappropriated, award exemplary damages in an amount not more than 2 times the amount of the damages awarded under subparagraph (B); and

(D) if a claim of the misappropriation is made in bad faith, which may be established by circumstantial evidence, a motion to terminate an injunction is made or opposed in bad faith, or the trade secret was willfully and maliciously misappropriated, award reasonable attorney's fees to the prevailing party.

## (c) Jurisdiction.—

The district courts of the United States shall have original jurisdiction of civil actions brought under this section.

## (d) Period of limitations.—

A civil action under subsection (b) may not be commenced later than 3 years after the date on which the misappropriation with respect to which the action would relate is discovered or by the exercise of reasonable diligence should have been discovered. For purposes of this subsection, a continuing misappropriation constitutes a single claim of misappropriation.

## (b) Definitions.—

Section 1839 of title 18, United States Code, is amended—

## (1) in paragraph (3)—

(A) in subparagraph (B), by striking "the public" and inserting "another person who can obtain economic value from the disclosure or use of the information"; and

(B) by striking "and" at the end;

(2) in paragraph (4), by striking the period at the end and inserting a semicolon; and

(3) by adding at the end the following:

## (5) the term "misappropriation" means—

(A) 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

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

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

(ii) at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was—

(I) derived from or through a person who had used improper means to acquire the trade secret;

(II) 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

(III) 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

(iii) before a material change of the position of the person, knew or had reason to know that—

(I) the trade secret was a trade secret; and

(II) knowledge of the trade secret had been acquired by accident or mistake;

## (6) the term "improper means"—

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

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

(7) the term "Trademark Act of 1946" means the Act entitled "An Act to provide for the registration and protection of trademarks used in commerce, to carry out the provisions of certain international conventions, and for other purposes, approved July 5, 1946 (15 U.S.C. 1051 et seq.) (commonly referred to as the 'Trademark Act of 1946' or the 'Lanham Act')".

## (c) Exceptions to prohibition.—

Section 1833 of title 18, United States Code, is amended, in the matter preceding paragraph (1), by inserting "or create a private right of action for" after "prohibit".

## (d) Conforming amendments.—

(1) The section heading for section 1836 of title 18, United States Code, is amended to read as follows:

**Sec. 1836. Civil proceedings**

(2) The table of sections for chapter 90 of title 18, United States Code, is amended by striking the item relating to section 1836 and inserting the following:

1836. Civil proceedings.

## (e) Effective date.—

The amendments made by this section shall apply with respect to any misappropriation of a trade secret (as defined in section 1839 of title 18, United States Code, as amended by this section) for which any act occurs on or after the date of the enactment of this Act.

## (f) Rule of construction.—

Nothing in the amendments made by this section shall be construed to modify the rule of construction under section 1838 of title 18, United States Code, or to preempt any other provision of law.

## (g) Applicability to other laws.—

This section and the amendments made by this section shall not be construed to be a law pertaining to intellectual property for purposes of any other Act of Congress.

**Sec. 3. Trade secret theft enforcement**

## (a) In general.—

Chapter 90 of title 18, United States Code, is amended—

(1) in section 1832(b), by striking "\$5,000,000" and inserting "the greater of \$5,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided"; and

(2) in section 1835—

(A) by striking "In any prosecution" and inserting the following:

(a) In general.—

In any prosecution

; and

(B) by adding at the end the following:

## (b) Rights of trade secret owners.—

The court may not authorize or direct the disclosure of any information the owner asserts to be a trade secret unless the court allows the owner the opportunity to file a submission under seal that describes the interest of the owner in keeping the information confidential. No submission under seal made under this subsection may be used in a prosecution under this chapter for any purpose other than those set forth in this section, or otherwise required by law. The provision of information relating to a trade secret to the United States or the court in connection with a prosecution under this chapter shall not constitute a waiver of trade secret protection, and the disclosure of information relating to a trade secret in connection with a prosecution under this chapter shall not constitute a waiver of trade secret protection unless the trade secret owner expressly consents to such waiver.

## (b) RICO predicate offenses.—

Section 1961(1) of title 18, United States Code, is amended by inserting "sections 1831 and 1832 (relating to economic espionage and theft of trade secrets)," before "section 1951".

**Sec. 4. Report on theft of trade secrets occurring abroad**

## (a) Definitions.—

In this section:

## (1) Director.—

The term "Director" means the Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office.

## (2) Foreign instrumentality, etc.—

The terms "foreign instrumentality", "foreign agent", and "trade secret" have the meanings given those terms in section 1839 of title 18, United States Code.

## (3) State.—

The term "State" includes the District of Columbia and any commonwealth, territory, or possession of the United States.

## (4) United States company.—

The term "United States company" means an organization organized under the laws of the United States or a State or political subdivision thereof.

## (b) Reports.—

Not later than 1 year after the date of enactment of this Act, and biannually thereafter, the Attorney General, in consultation with the Intellectual Property Enforcement Coordinator, the Director, and the heads of other appropriate agencies, shall submit to the Committees on the Judiciary of the House of Representatives and the Senate, and make publicly available on the Web site of the Department of Justice and disseminate to the public through such other means as the Attorney General may identify, a report on the following:

- (1) The scope and breadth of the theft of the trade secrets of United States companies occurring outside of the United States.
- (2) The extent to which theft of trade secrets occurring outside of the United States is sponsored by foreign governments, foreign instrumentalities, or foreign agents.
- (3) The threat posed by theft of trade secrets occurring outside of the United States.
- (4) The ability and limitations of trade secret owners to prevent the misappropriation of trade secrets outside of the United States, to enforce any judgment against foreign entities for theft of trade secrets, and to prevent imports based on theft of trade secrets overseas.
- (5) A breakdown of the trade secret protections afforded United States companies by each country that is a trading partner of the United States and enforcement efforts available and undertaken in each such country, including a list identifying specific countries where trade secret theft, laws, or enforcement is a significant problem for United States companies.
- (6) Instances of the Federal Government working with foreign countries to investigate, arrest, and prosecute entities and individuals involved in the theft of trade secrets outside of the United States.
- (7) Specific progress made under trade agreements and treaties, including any new remedies enacted by foreign countries, to protect against theft of trade secrets of United States companies outside of the United States.
- (8) Recommendations of legislative and executive branch actions that may be undertaken to—



- (A) reduce the threat of and economic impact caused by the theft of the trade secrets of United States companies occurring outside of the United States;
- (B) educate United States companies regarding the threats to their trade secrets when taken outside of the United States;
- (C) provide assistance to United States companies to reduce the risk of loss of their trade secrets when taken outside of the United States; and
- (D) provide a mechanism for United States companies to confidentially or anonymously report the theft of trade secrets occurring outside of the United States.

#### Sec. 5. Sense of Congress

It is the sense of Congress that—

- (1) trade secret theft occurs in the United States and around the world;
- (2) trade secret theft, wherever it occurs, harms the companies that own the trade secrets and the employees of the companies;
- (3) chapter 90 of title 18, United States Code (commonly known as the "Economic Espionage Act of 1996"), applies broadly to protect trade secrets from theft; and
- (4) it is important when seizing information to balance the need to prevent or remedy misappropriation with the need to avoid interrupting the—
  - (A) business of third parties; and
  - (B) legitimate interests of the party accused of wrongdoing.

#### Sec. 6. Best practices

(a) In general.—

Not later than 2 years after the date of enactment of this Act, the Federal Judicial Center, using existing resources, shall develop recommended best practices for—

- (1) the seizure of information and media storing the information; and
- (2) the securing of the information and media once seized.

(b) Updates.—

The Federal Judicial Center shall update the recommended best practices developed under subsection (a) from time to time.

(c) Congressional submissions.—

The Federal Judicial Center shall provide a copy of the recommendations developed under subsection (a), and any updates made under subsection (b), to the—

- (1) Committee on the Judiciary of the Senate; and
- (2) Committee on the Judiciary of the House of Representatives.

#### Sec. 7. Immunity from liability for confidential disclosure of a trade secret to the government or in a court filing

(a) Amendment.—

Section 1833 of title 18, United States Code, is amended—

- (1) by striking "This chapter" and inserting "(a) In general.—This chapter";
- (2) in subsection (a)(2), as designated by paragraph (1), by striking "the reporting of a suspected violation of law to any governmental entity of the United States, a State, or a political subdivision of a State, if such entity has lawful authority with respect to that violation" and inserting "the disclosure of a trade secret in accordance with subsection (b)"; and
- (3) by adding at the end the following:

(b) Immunity from liability for confidential disclosure of a trade secret to the Government or in a court filing.—

(1) Immunity.—

An individual shall 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.

(2) Use of trade secret information in anti-retaliation lawsuit.—

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—

(A) files any document containing the trade secret under seal; and

(B) does not disclose the trade secret, except pursuant to court order.

(3) Notice.—

(A) In general.—

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.

(B) Policy document.—

An employer shall be considered to be in compliance with the notice requirement in subparagraph (A) if the employer provides a cross-reference to a policy document provided to the employee that sets forth the employer's reporting policy for a suspected violation of law.

(C) Non-compliance.—

If an employer does not comply with the notice requirement in subparagraph (A), the employer may not be awarded exemplary damages or attorney fees under subparagraph (C) or (D) of section 1836(b)(3) in an action against an employee to whom notice was not provided.

(D) Applicability.—

This paragraph shall apply to contracts and agreements that are entered into or updated after the date of enactment of this subsection.

(4) Employee defined.—

For purposes of this subsection, the term "employee" includes any individual performing work as a contractor or consultant for an employer.

(5) Rule of construction.—

Except as expressly provided for under this subsection, nothing in this subsection shall be construed to authorize, or limit liability for, an act that is otherwise prohibited by law, such as the unlawful access of material by unauthorized means.

(b) Technical and conforming amendment.—

Section 1838 of title 18, United States Code, is amended by striking "This chapter" and inserting "Except as provided in section 1833(b), this chapter".

*Speaker of the House of Representatives.*

*Vice President of the United States and President of the Senate.*

[site MENU](#)

[Home \(/\)](#)

[Start Tracking \(/start\)](#)

[About GovTrack \(/about\)](#)

[Data/API \(/developers\)](#)

[Privacy & Legal \(/legal\)](#)

[Log in \(/accounts/login\)](#)

follow GOVTRACK

**f** [Facebook \(https://www.facebook.com/govtrack/\)](https://www.facebook.com/govtrack/)

**t** [Twitter \(http://twitter.com/govtrack\)](http://twitter.com/govtrack)

**M** [Medium \(https://medium.com/govtrack-insider\)](https://medium.com/govtrack-insider)

**📝** [Blog \(/blog\)](#)

**🔗** [Code \(https://github.com/govtrack/govtrack.us-web/commits/master\)](https://github.com/govtrack/govtrack.us-web/commits/master)

Launched in 2004, GovTrack helps everyone learn about and track the activities of the United States Congress. This is a project of [Civic Impulse, LLC \(http://www.civicimpulse.com\)](http://www.civicimpulse.com). GovTrack.us is not a government website.

[About the Site \(/about\)](#) | [Contact Us \(/contact\)](#)

You are encouraged to reuse any material on this site. GovTrack supports other Congress-tracking websites through our [open data \(/developers\)](#).

108 A.D.2d 991  
Supreme Court, Appellate Division, Third  
Department, New York.

DELTA FILTER CORPORATION,  
Appellant-Respondent,  
v.  
Gilles A. MORIN et al., Respondents-Appellants.

Feb. 14, 1985.

Employees of filter manufacturing firm left and formed a competing corporation and former employer brought action alleging misappropriation of trade secrets. Former employees counterclaimed alleging trade defamation and interference with business relationships. The Supreme Court, Trial Term, Saratoga County, Ford, J., dismissed complaint at the close of former employer's case and dismissed counterclaims at close of all proof, and both parties appealed. The Supreme Court, Appellate Division, held that: (1) evidence was sufficient to find machinery and processor of former employer did not merit trade secret protection, and (2) actions of former employer in informing customers and suppliers that former employees had founded their own firm and there was litigation between the two did not constitute trade defamation or interference in business relationships.

Affirmed.

West Headnotes (5)

- [1] **Antitrust and Trade Regulation**  
⚡What Are "Trade Secrets" or Other Protected Proprietary Information, in General

"Trade secret" protected from misappropriation is a formula, process, device or compilation of information used in one's business which confers a competitive advantage over those in similar businesses who do not know or use it.

16 Cases that cite this headnote

- [2] **Antitrust and Trade Regulation**  
⚡Necessity That Information Be Secret  
**Antitrust and Trade Regulation**  
⚡Vigilance in Protecting Secret; Abandonment or Waiver

Essential requisite to legal protection against misappropriation of a trade secret is the element of secrecy; secrecy can mean substantial exclusivity of the trade secret or employment of precautionary measures to preserve exclusive knowledge.

8 Cases that cite this headnote

- [3] **Antitrust and Trade Regulation**  
⚡Weight and Sufficiency of Evidence

In action by filter manufacturer alleging misappropriation of trade secrets by use of similar manufacturing machinery in corporation set up by former employees, testimony that other manufacturers of various kinds of filters used similar equipment, much of the equipment was sold on the open market, and testimony that only distinctive feature of manufacturing process was of dubious significant competitive advantage was sufficient to support finding that process was not entitled to trade secrecy protection.

4 Cases that cite this headnote

- [4] **Antitrust and Trade Regulation**  
⚡Weight and Sufficiency of Evidence

In action for misappropriation of trade secrets, testimony that machines employed could be duplicated without blueprints or photographs by simply describing them to an experienced machinist, lack of rudimentary precautions to prevent employees from acquiring familiarity with the machines or later using the knowledge thus acquired, and inspections by competitors was sufficient to support finding that neither machinery nor process was so distinctive or

secret as to merit protection.

2 Cases that cite this headnote

[5]

### Libel and Slander

☞ Nature and Elements in General

### Torts

☞ Business Relations or Economic Advantage, in General

Actions by manufacturer in informing customers and suppliers that principal employees who had formed a competing corporation were no longer employed by it and that there was litigation between the two companies was not sufficient to constitute trade defamation or interference with business relationships of the newly established corporation.

1 Cases that cite this headnote

### Attorneys and Law Firms

**\*\*143** Nolan & Heller, Albany (Mark L. Heller, Albany, of counsel), for appellant-respondent.

Miller & Williams, Clifton Park (G. Kimball Williams, Clifton Park, of counsel), for respondents-appellants.

**\*\*144** Before MAHONEY, P.J., and KANE, CASEY and WEISS, JJ.

### Opinion

PER CURIAM.

Cross appeals from a judgment of the Supreme Court, entered January 18, 1984 in Saratoga County, upon a decision of the court at Trial Term, without a jury.

In 1975, plaintiff, Delta Filter Corporation (Delta), purchased the filtration division of a Schenectady-based environmental research and development company known as Environment One Corporation, including its machinery and equipment for producing high efficiency particulate air (HEPA) filters. Simultaneously, various Environment

One Corporation personnel transferred their employment to Delta, among whom was defendant Gilles Morin, who was put in charge of Delta's HEPA filter production. Morin, defendant Thomas Pratt (another Delta employee) and Harry Grounds incorporated defendant Northland Filter Systems, Inc. (Northland) in April 1981; two months later, Morin resigned from Delta.

When Northland then went into competition with Delta in the production and sale of HEPA filters, Delta commenced the instant action for an injunction and damages. The action was **\*992** based on allegations that Northland had misappropriated Delta's trade secrets by using identical machine components and processes in producing HEPA filters and by taking over its customer lists. The latter claim was subsequently abandoned, however. Northland counterclaimed for damages, based upon allegations of Delta's trade defamation and interference with Northland's business relationships with its suppliers and customers. After a nonjury trial, Trial Term dismissed the complaint at the close of plaintiff's case and the counterclaims of the close of all the proof. These cross appeals ensued.

In dismissing the complaint, Trial Term found that the three principal manufacturing components of Northland's production of HEPA filters were substantially identical to those of Delta's, namely, the pleater which folds the filter or media paper into accordion pleats, a corrugator which imparts an image into aluminum separators between the pleats, and a dual saw used to cut and trim the filter's particle board frame. Trial Term nevertheless ruled against Delta on the ground that neither Delta's equipment nor its production process was of such a nature as to attain the status of a trade secret. Our review of the record leads us to conclude that Trial Term was correct in its assessment.

[1] [2] New York has substantially adopted the approach of the original Restatement of Torts (1939) to the law of trade secrets (*Eagle Comtronics v. Pico, Inc.*, 89 A.D.2d 803, 804, 453 N.Y.S.2d 470, *lv. denied* 58 N.Y.2d 601, 458 N.Y.S.2d 1025, 444 N.E.2d 1012; *Ferranti Elec. v. Harwood*, 43 Misc.2d 533, 539, 251 N.Y.S.2d 612; *Minnesota Min. & Mfg. Co. v. Technical Tape Corp.*, 23 Misc.2d 671, 678-679, 192 N.Y.S.2d 102, *affd.* 15 A.D.2d 960, 226 N.Y.S.2d 1021, *affd.* 18 A.D.2d 679, 235 N.Y.S.2d 830). Under the rationale of the Restatement, a trade secret is generally defined as a formula, process, device or compilation of information used in one's business which confers a competitive advantage over those in similar businesses who do not know or use it (Restatement of Torts § 757 comment b [1939]). An essential requisite to legal protection against

misappropriation of such a formula, process, device or compilation of information is the element of secrecy. Secrecy is used in the Restatement in two related senses: (1) as substantial exclusivity of knowledge of the formula, process, device or compilation of information (“Matters of public knowledge or of general knowledge in an industry cannot be appropriated by one as his secret” [*id.*] ); and (2) as the employment of precautionary measures to preserve such exclusive knowledge by limiting legitimate access by others (“Nevertheless, a substantial element of secrecy must exist, so that, except by the use of improper means, there would be difficulty in acquiring the information” [*id.*] ).

**\*\*145** <sup>[31]</sup> Regarding the element of secrecy in the first of the foregoing connotations, Trial Term held that Delta failed to prove that its **\*993** filter production process was materially different from those of its competitors, or that its equipment was generally unavailable and not easily assembled. The record amply supports that conclusion. Northland’s expert testified, and in some instances demonstrated by comparison photographs, that other manufacturers of various kinds of filters use pleating equipment similar to Delta’s and thereby produce similar results; that sellers of HEPA filter manufacturing equipment marketed corrugating machines similar in composition, design and function to Delta’s and Northland’s; and that the double-saw trimming device was sold on the open market and was in use at the plants of several competitors. Even Delta’s expert acknowledged that the only distinctive feature of the entire Delta filter manufacturing process was its pleater. As Trial Term stated, however, it was dubious as to the degree to which Delta’s method of pleating the filter gave it any significant competitive advantage.

<sup>[41]</sup> The proof of Delta’s precautions to safeguard its process and equipment from public disclosure by all but improper means was equally unpersuasive on the secrecy element of its claim. According to an engineering consultant employed exclusively by Delta, the machines at issue could be duplicated without blueprints or photographs by simply describing them from memory to an experienced machinist. This corroborated Northland’s witnesses regarding the basic technique through which Northland was able to reproduce its devices. Yet Delta failed to take rudimentary precautions to prevent employees from acquiring familiarity with the machines during their work, or later using the knowledge thus acquired after leaving the company. Delta’s president also

admitted that its filter production process and devices were open to inspection from time to time by representatives of its competitors. Although Delta’s president testified to restrictions on access to blueprints, this conflicted with the testimony of other witnesses, thus merely creating an issue of credibility which Trial Term was in the best position to resolve (*see Huertas v. State of New York*, 84 A.D.2d 650, 651, 444 N.Y.S.2d 307).

In short, Delta failed to sustain its burden of proof that the process or machines used in producing HEPA filters was significantly distinctive or secret so as to merit trade secrecy protection. Likewise, particularly in the absence of any secrecy agreement preventing defendants Morin and Pratt from using the technical knowledge which they naturally and legitimately acquired during their employment, the credible evidence does not support any inference that they used improper means to acquire the information necessary to reproduce Delta’s processes and equipment, or that such means were necessary to do so. Here, as **\*994** in *Ferranti Elec. v. Harwood*, 43 Misc.2d 533, 251 N.Y.S.2d 612, *supra*, the actions of the individual defendants were “as consistent with the normally expected desire for fair, economic self-improvement as they [were] with a well-planned, well-concealed conspiratorial attempt at industrial piracy” (*id.* at 541–542, 251 N.Y.S.2d 612). Accordingly, Trial Term correctly dismissed the complaint.

<sup>[5]</sup> Regarding defendants’ counterclaims, the record is devoid of any proof of Delta’s counteractions against Northland other than informing customers and suppliers that the Northland principals were no longer employed by Delta and that there was litigation between the two companies. Since such statements in no way establish an actionable claim for defamation, unfair competition or tortious interferences with business relationships, the counterclaims were also properly dismissed.

For all of the foregoing reasons, the judgment should be affirmed.

Judgment affirmed, without costs.

#### Parallel Citations

108 A.D.2d 991, 485 N.Y.S.2d 143



29 N.Y.2d 387  
Court of Appeals of New York.

LEO SILFEN, INC., et al., Respondents,  
v.  
Maurice C. CREAM et al., Appellants, et al.,  
Defendant.

Jan. 12, 1972.

Action for damages and to enjoin discharged employee from soliciting former employers' customers. Following order of the Appellate Division of the Supreme Court in the Second Judicial Department, affirming judgment of the Supreme Court, Westchester County, Special Term, Frank S. McCullough, J., in favor of employers on issue of liability and granting injunctive relief, the Supreme Court, Westchester County, entered judgment from which appeal was taken. The Court of Appeals, Breitel, J., held that where former employee was not shown to have appropriated by copying, studied memory, or some other means detailed information in employers' customer files, and where employers' customers were likely, if not known, users of employers' building maintenance supplies and engaged in business at advertised locations, so that their names and addresses could readily be found by those engaged in employers' trade and so that employers' investment and its customer lists reflected simply a widespread canvassing of an obvious and highly competitive market, the names of the customers alone involved no trade secret and no wrongful conduct by employee was shown by circumstance that he had solicited 47 of 1,100 customers appearing on list prepared by employers from their confidential files.

Judgment reversed; complaint dismissed.

West Headnotes (5)

[1] **Labor and Employment**  
☞Customer information

Where former employee was not shown to have appropriated by copying, studied memory, or some other means detailed information in employers' customer files, and where employers' customers were likely, if not known, users of employers' merchandise and engaged in

business at advertised locations, the names of the customers alone involved no trade secret and no wrongful conduct by employee was shown by circumstance that he had solicited 47 of 1,100 customers appearing on list prepared by employers from their confidential files.

58 Cases that cite this headnote

[2] **Injunction**  
☞Disclosure or use of trade secrets or confidential information

If there has been a physical taking or studied copying of customer lists by employee, court may in proper case enjoin solicitation, not necessarily as violation of a trade secret, but as breach of trust and confidence. Penal Law 1965, § 250.25.

29 Cases that cite this headnote

[3] **Antitrust and Trade Regulation**  
☞Employer and employee

If there have been wrongful or fraudulent tactics employed by former employee in connection with solicitation of employers' customers, a court may award damages and enjoin further similar conduct as constituting unfair competition.

6 Cases that cite this headnote

[4] **Antitrust and Trade Regulation**  
☞Customer lists and information  
**Injunction**  
☞Disclosure or use of trade secrets or confidential information  
**Labor and Employment**  
☞Customer information



Generally, where customers are readily ascertainable outside employers' business as prospective users of employers' services or products, trade secret protection will not attach and courts will not enjoin former employee from soliciting employers' customers, but customer lists and files will be protected as trade secrets if they are not known in the trade or are discoverable only by extraordinary efforts, particularly where patronage has been secured by years of effort and advertising.

95 Cases that cite this headnote

<sup>[5]</sup> **Injunction**

Disclosure or use of trade secrets or confidential information

In absence of express agreement to that effect between the parties, or demonstration that a customer list has the attributes of a trade secret, courts should not enjoin exemployee from engaging in fair and open competition with his former employer.

17 Cases that cite this headnote

**Attorneys and Law Firms**

\*\*\*424 \*\*637 \*388 Alvin I. Goidel, New York City, for appellants.

Martin L. Conrad and Herbert L. Finkelstein, New York City, for respondents.

**Opinion**

\*389 BREITEL, Judge.

In an action for damages and to enjoin a discharged employee from soliciting his former employers' customers, defendants appeal. The \*\*\*425 issue is whether the employers' investment of time and money in accumulating a list of approximately 15,000 customers, most being readily ascertainable in the trade as likely

users of plaintiffs' services, entitles the list to trade secret protection.

After a nonjury trial, the court concluded that the list of customers and catalogue of customer data were trade secrets, and enjoined defendants from doing business with any of plaintiffs' customers. The Appellate Division 37 A.D.2d 721, 323 N.Y.S.2d 1018, affirmed with two Justices dissenting.

<sup>[1]</sup> The judgment should be reversed and the complaint dismissed. Plaintiffs have failed to prove a physical appropriation or copying of confidential information, or wrongful disclosure or use of a trade secret. In particular, no trade secret protection is warranted since plaintiffs' customers are likely, if not known, users of the employers' merchandise and engaged in business at advertised locations.

Plaintiff corporations are engaged in selling building maintenance supplies to industrial and commercial users. Plaintiffs purchase their inventory from independent supply houses and then, at a substantial markup, resell to customers under their own label. Plaintiff Silfen sells soaps, polishes, waxes, finishers, and disinfectants, \*\*638 while plaintiff Formula 33 Corporation specializes in ice and snow melting compounds.

In 1949 defendant Cream joined Silfen, then engaged only in the paper and twine business. Cream was assigned and became solely responsible for the development of a cleaning and maintenance chemical supply division. During its formative years Cream interviewed and hired salesmen, developed products, and found suppliers. Initial customer solicitation consisted of direct contact and media advertising. Meeting little success he employed the services of mailing houses which provided lists \*390 of prospects to whom brochures and business reply cards were forwarded. Eventually, an average of one million mailings were made annually with a reply rate of 0.6%. Of those replying 25% Became customers at an average cost per new customer in 1967 of \$45. Over the years, some 15,000 customers were obtained.

For each customer a separate file was kept containing: name of purchasing agent and other personnel at customer's office; temperament of purchasing agent; gratuities given; particular requirements; and past purchases. In 1961 these customer profiles were consolidated into a central filing system and measures were taken to insure that each salesman had access only to that portion of the files containing his customers. So concerned were plaintiffs in the protection of this information that in the employment agreement with each salesman hired after 1961 it was provided: '(The

salesman) acknowledges that \*\*\*426 the list of the Corporations' customers is a unique asset of their respective businesses, and \* \* \* will not, during or after the term of his employment, appropriate to his own use or disclose to others for any purpose, any names on such list or any confidential information obtained by him during his employment.' Vigilance is also demonstrated by a form required to be signed by each salesman after contact with a customer: 'The names of all the company customers ever called by me, and those appearing on the face of this telephone report sheet, were obtained from leads furnished by the company and remain the property of the company and will not be disclosed to any unauthorized persons in violation of the trust placed in me by the company.'

In 1965, on the death of the principal of Silfen and the taking of control by his widow, Cream was named executive vice-president and general manager of plaintiff corporations for a term of 12 years. The written agreement between the parties provided for a base salary of \$26,000 plus 25% Of the aggregate net profits. The corporations reserved the right to discharge Cream if the aggregate net profits in any one year failed to exceed \$35,000. It was also provided that if Cream terminated the agreement he would 'not, for one year thereafter \* \* \* engage in the sale to the corporations' customers of any products \*391 competing with the corporations' products.' Since Cream was discharged this restriction is not controlling. The agreement contained no comparable provision to cover Cream's discharge.

On November 17, 1967, Cream was discharged purportedly because of a decline in net profits. Cream, however, urges that he was discharged in order to make room for the new husband of the widow, the former Mrs. Silfen. Thirteen days after his discharge he set up Real Estate Maintenance Chemical Specialty Corporation and engaged in the same business as plaintiffs except limited to building owners and building managers. About three months later, in March, 1968, plaintiffs brought this action to enjoin defendants' solicitation of plaintiffs' customers. The complaint alleged that defendants had been soliciting plaintiffs' customers, that Cream had made copies of plaintiffs' secret and confidential customer files, and was using such information in his solicitation. Cream admits that of a list of 1,100 customers submitted by plaintiffs defendants had solicited 47. Defendants, however, contend that the names of these customers \*\*639 were procured from available commercial lists compiled by commercial list houses. Defendants allege in their answer and assert in their testimony that the customers are openly engaged in business at advertised locations and their names are well known to plaintiffs' competitors.

[2] [3] Notably, plaintiffs did not attempt to sustain their allegation that Cream had made copies of plaintiffs' secret and confidential files, \*\*\*427 or used the recorded detail in those files with respect to each customer's 'profile'. The solicitation of plaintiffs' customers was at most the product of casual memory, or, as defendants would have the court believe, coincidence.<sup>1</sup> If there has been \*392 a physical taking or studied copying, the court may in a proper case enjoin solicitation, not necessarily as a violation of a trade secret, but as an egregious breach of trust and confidence while in plaintiffs' service (Scott & Co. v. Scott, 186 App.Div. 518, 524—525, 174 N.Y.S. 583, 586—587; Ann., Customer List—As Trade Secret—Factors, 28 A.L.R.3d 7, pp. 120—124; 36 N.Y.Jur., Master and Servant, s 75; cf. Duane Jones Co. v. Burke, 306 N.Y. 172, 187—188, 117 N.E.2d 237, 244—245; Bruno Co. v. Friedberg, 21 A.D.2d 336, 339—340, 250 N.Y.S.2d 187, 190—191; former Penal Law, s 553, subd. 6). Nor is there any allegation or evidence of other wrongful or fraudulent tactics employed by Cream in connection with the solicitation of plaintiffs' customers. If there had been, a court might award damages and enjoin further similar conduct as constituting unfair competition. (Scott & Co. v. Scott, Supra, 186 App.Div. at p. 525, 174 N.Y.S. at p. 587; Ann., 28 A.L.R.3d, Supra, at pp. 128—129; 60 N.Y.Jur., Trademarks, Tradenames, and Unfair Competition, s 127.) All that remains, therefore, on the theory alleged in the complaint or developed on the trial is whether plaintiffs' customer list, exclusive of the recorded detail about each customer, classifies as a trade secret rendering defendants' solicitation of customers on that list improper, sufficient to warrant injunction and damages.

[4] Generally, where the customers are readily ascertainable outside the employer's business as prospective users or consumers of the employer's services or products, trade secret protection will not attach and courts will not enjoin the employee from soliciting his employer's customers (Boosing v. Dorman, 148 App.Div. 824, 827, 133 N.Y.S. 910, 911, affd. 210 N.Y. 529, 103 N.E. 1121; Tepfer & Sons v. Zschaler, 25 A.D.2d 786, 787, 269 N.Y.S.2d 552; Hudson Val. Propane Corp. v. Byrne, 24 A.D.2d 908, 909, 264 N.Y.S.2d 416, 417; Abdallah v. Crandall, 273 App.Div. 131, 133—134, 76 N.Y.S.2d 403, 405—406; \*\*\*428 Goldberg v. Goldberg, 205 App.Div. 435, 438—439, 200 N.Y.S. 3, 6—7; Scott & Co. v. Scott, Supra, 186 App.Div. at pp. 524—525, 527, 174 N.Y.S. at pp. 586—587, 588; McLean v. Hubbard, 24 Misc.2d 92, 96—97, 194 N.Y.S.2d 644, 648—649, affd. 11 A.D.2d 1084, 208 N.Y.S.2d 443; 60 N.Y.Jur., Trademark, Tradenames and Unfair Competition, s 113; 2 Callmann, Unfair Competition, Trademarks and Monopolies (3d ed.), s 54.2(c)(2), pp.

434—449, esp. 443; Ann., Customer List—As Trade Secret—Factors, \*\*640 28 A.L.R.3d 7, s 10, subd. (b), Supra; as to trade secrets generally see Restatement, Torts, s 757). Conversely, where the customers are not known in the trade or are discoverable only by extraordinary efforts courts have not hesitated to \*393 protect customer lists and files as trade secrets. This is especially so where the customers' patronage had been secured by years of effort and advertising effected by the expenditure of substantial time and money (Town & Country House & Home Serv. v. Newbery, 3 N.Y.2d 554, 558—559, 170 N.Y.S.2d 328, 331—332, 147 N.E.2d 724, 726—727; Cupid Diaper Serv. v. Adelman, 27 Misc.2d 1095, 1096, 211 N.Y.S.2d 813, 814; 2 Callmann, Op. cit., supra, p. 447 and cases cited; 36 N.Y.Jur., Master and Servant, s 76, p. 505, cf. Hudson Val. Propane Corp. v. Byrne, Supra, 24 A.D.2d at p. 909, 264 N.Y.S.2d at p. 417; Witkop & Holmes Co. v. Boyce, 61 Misc. 126, 131, 112 N.Y.S. 874, 877, affd. 131 App.Div. 922, 115 N.Y.S. 1150).

The customers solicited by defendants, as apparently found by the trial court, are openly engaged in business in advertised locations and their names and addresses may readily be found by those engaged in the trade. Indeed, plaintiffs' counsel apparently conceded as much at the conclusion of the trial, but thought that circumstance irrelevant unless defendants had actually obtained the prospects from commercially available lists and not from Cream's prior service with plaintiffs. Relying upon this court's opinion in Town & Country House & Home Serv. v. Newbery, 3 N.Y.2d 554, 170 N.Y.S.2d 328, 147 N.E.2d 724, Supra, the trial court apparently believed that commercial notoriety of defendant's prospects as users of this type of service is not controlling, misapplying, it is suggested, the Town & Country case to make an exception where there has been substantial effort by plaintiffs in acquiring their patronage.

Indeed, the Town & Country case presents an interesting contrast. Plaintiff in that case was engaged in the business of house and home cleaning by contract with individual householders. After three years of operation it had acquired 240 customers. Defendants left its employment, established a competing corporation, and solicited 38 of plaintiff's customers. Only plaintiff's customers were solicited. The court marked the type of customer that the parties serviced.

\*\*\*429 '(T)he customers of plaintiff were not and could not be obtained merely by looking up their names in the telephone or city directory or by going to any advertised locations, but had to be screened from among many other housewives who did not wish services such as respondent

and appellants were equipped to render, but preferred to do their own housework. In most instances housewives do their own house cleaning. \*394 The only appeal which plaintiff could have was to those whose cleaning had been done by servants regularly or occasionally employed, except in the still rarer instances where the housewife was on the verge of abandoning doing her own work by hiring some outside agency.' (3 N.Y.2d at p. 559, 170 N.Y.S.2d, at p. 332, 147 N.E.2d, at p. 726).

'It would be different if these customers had been equally available to appellants and respondent, but, as has been related, these customers had been screened by respondent at considerable effort and expense, without which their receptivity and willingness to do business with this kind of a service organization could not be known.' (Id., at p. 560, 170 N.Y.S.2d, at p. 333, 147 N.E.2d, at p. 727).

Unlike the customers in the Town & Country case (supra), plaintiffs' customers were readily ascertainable as likely prospects. Although plaintiffs have demonstrated an investment of time and money in developing a patronage of approximately 15,000 enterprises, the investment was not an attempt to create a market for a new type of service as was the case in the \*\*641 Town & Country case. Rather, that investment reflected simply widespread canvassing of an obvious and highly competitive market. Indeed, consider the comparable investment in the distribution of soap and soap products to the individual consumer.

A better parallel than the Town & Country case is Abdallah v. Crandall, 273 App.Div. 131, 76 N.Y.S.2d 403, Supra. In Abdallah the plaintiff employer was engaged in the dairy business and the defendant employee made deliveries on some of plaintiff's retail milk routes. When the defendant left plaintiff's employment, he joined a competing business and solicited his former customers. In dismissing the former employer's action to enjoin such solicitation, the court noted; 'In some instances a list of customers may be a trade secret but it would be straining the meaning of the word beyond any reasonable limit to hold that the list transferred in this case came within that category. The plaintiff himself conceded on the trial of the action that every householder in both of the communities involved either bought milk or was a potential customer for it. It was also conceded, \*\*\*430 and it is a matter of common knowledge, that the delivery of milk from the very nature of the business is open and notorious. A trade secret, like any other secret, is nothing more than private matter; something known to only one or a few and kept from the general public; \*395 and not susceptible to general knowledge. Kaumagraph Co. v. Stampagraph Co., 235 N.Y. 1, 138 N.E. 485. A list of milk customers in a small city like Cortland, and a village like Homer, hardly

meets such a definition. We are therefore constrained to hold with the referee that the list of Brown's milk customers was not a trade secret according to the accepted meaning of that term.' (pp. 133—134, 76 N.Y.S.2d, at p. 406).

<sup>151</sup> In the absence of express agreement to that effect between the parties, or a demonstration that a customer list has the several attributes of a trade secret, courts, without more, should not enjoin an ex-employee from engaging in fair and open competition with his former employer. The limiting effects upon the former employee with respect to his ability to earn a living are marked and obvious. (Cf. *Purchasing Assoc. v. Weitz*, 13 N.Y.2d 267, 272, 246 N.Y.S.2d 600, 603, 196 N.E.2d 245, 247; *Paramount Pad Co. v. Baumrind*, 4 N.Y.2d 393, 175 N.Y.S.2d 809, 151 N.E.2d 609.) Moreover, the issuance of the permanent injunction in the present case has an untoward consequence. By discharging Cream plaintiffs obtained greater protection than they would have had under their agreement with him, if he had terminated the employment. It was observed earlier that the 1965 employment agreement provided that Cream would not solicit plaintiffs' customers for one year following his termination of the employment. This provision suggests that the parties considered Cream's role as a future competitor, and, more important, were satisfied to provide protection for only one year.

In concluding, it may be stated expressly what was earlier implied, namely, that if defendants had been shown to have appropriated by copying, studied memory, or by

#### Footnotes

<sup>1</sup> In passing it should be noted that defendants do not argue that otherwise protectible information might be exempted if it is shown that the employee's appropriation was the result of experience or memory and not physical taking or copying. There are authorities which suggest that an employee may use in competition with his former employer the names, even lists, of customers retained in his memory (see Restatement, 2d, Agency, s 396, Comment b; *Federal Laundry Co. v. Zimmerman*, 218 Mich. 211, 214, 187 N.W. 335; *Grand Union Tea Co. v. Dodds*, 164 Mich. 50, 54—55, 128 N.W. 1090; contra, *People's Coat, Apron & Towel Supply Co. v. Light*, 171 App.Div. 671, 157 N.Y.S. 15, affd. 224 N.Y. 727, 121 N.E. 886; *United Ins. Co. v. Dienno, D.C.*, 248 F.Supp. 553; *Van Prods. Co. v. General Weld. & Fabricating Co.*, 419 Pa. 248, 262—263, 213 A.2d 769; *Colonial Laundries v. Henry*, 48 R.I. 332, 336—338, 138 A. 47, see, generally, Ann., *Customer List—As Trade Secret—Factors*, 28 A.L.R.3d 7, at pp. 66—77).

some other manner which does not now come to mind, the detailed information in the customer files there would be a case quite different from this. The record shows no such appropriation with respect to a single customer, let alone many customers to an extent barring reliance on casual memory. Instead, it shows that defendants solicited 47 of the 1,100 customers submitted on a list prepared by plaintiffs from its confidential files. The point is that in the circumstances described names of customers alone involved no trade secret and there was no wrongful conduct by defendants. If \*\*\*431 trade secrets there were, they consisted of the data in the carefully secured and segregated files.

\*\*642 \*396 Accordingly, the judgment appealed from should be reversed and the complaint dismissed, with costs in all courts.

FULD, C.J., and BURKE, SCILEPPI, BERGAN, JASEN and GIBSON, JJ., concur.

Judgment reversed, etc.

#### Parallel Citations

29 N.Y.2d 387, 278 N.E.2d 636, 328 N.Y.S.2d 423



# Bond

## Trade Secret Protection Audit

*Prepare • Prevent • Protect*



*Commitment • Service • Value • Our Bond*

ALBANY BUFFALO GARDEN CITY ITHACA NEW YORK CITY OSWEGO ROCHESTER SYRACUSE UTICA NAPLES, FL OVERLAND PARK, KS

# We Help You Operate From a Position of Strength

All too often, companies react to trade secret theft rather than prepare for, or even prevent it. It is far more cost effective to protect your assets and prevent theft in the first place through the implementation of upgraded security measures and protocols and well drafted employment agreements.

*A Trade Secret Protection Audit will help put your company in a position of strength by, among other things:*

- *updating and enhancing your non-compete, non-solicit, and non-disclosure agreements;*
- *reviewing and fine-tuning your physical and digital security measures; and*
- *developing and implementing employee departure protocols.*

*The tiers of service (which can be customized) are as follows:*

## *Tier One:*

1. Analyze trade secrets and other protectable information and intangible assets.
2. Collaborate with your management to identify employees/contractors (a) with access to trade secrets; (b) who have developed relationships with key customers; and/or (c) who are otherwise considered key employees.
3. Analyze existing agreements for employees/contractors identified in paragraph 2 and, with respect to each such agreement:
  - a. Review and, where appropriate, update nondisclosure and/or confidentiality provisions in employment/contractor agreements.
  - b. Review and, where appropriate, update non-competition provisions in employment/contractor agreements.
  - c. Review and, where appropriate, update non-solicitation provisions in employment/contractor agreements.
  - d. Review and, where appropriate, update standard intellectual property assignment provisions in employment/contractor agreements.
  - e. Review and, where appropriate, update remedies provisions in employment/contractor agreements.
  - f. Review and, where appropriate, update employment/contractor agreements to ensure compliance with Defend Trade Secrets Act notice requirements.
4. Analyze standard third party confidentiality agreements.
5. Analyze existing policies/procedures to protect trade secret information.

## *Tier Two:*

*All items in tier one, plus:*

1. Preparation of any necessary agreements not already in existence.
2. Preparation of employee document preservation instructions template.
3. Draft trade secret protection policy.

*Looking for creativity,  
proactivity, experience,  
and knowledge?  
Look to Bond.*

# *Prepare • Prevent • Protect*

Following a complimentary meeting with members of executive management to evaluate the scope of company operations and discern areas of risk relative to trade secrets and intangible assets, our attorneys will prepare a summary recommending the next steps your company should consider taking. We will then provide you a customized quote for the costs to you for those services, which will be based not only on the scope of services you choose, but also the size of your company and the number of employees directly involved in the trade secrets context. Simply put, you will know exactly what you will pay for your trade secret protection audit before we start work.

### *Tier Three:*

#### **All items in tier two, plus:**

1. Audit of relevant human resources policies and procedures and, as relevant, employee manuals and employee training with respect to trade secret polices.
2. Human resources training on establishing trade secret protection with respect to the following topics:
  - a. Recruitment/hiring practices;
  - b. Employee departure and exit interview practices; and
  - c. Treatment of former employee's workspace, laptop, mobile devices, etc.

### *Tier Four:*

#### **All items in tier three, plus:**

1. Forensic audit of electronic security policies and protocols.\*
2. Coordination of forensic audit and, where appropriate, coordinate and assist in the implementation of new security policies and procedures.
  - \* *Forensic analysis services will be conducted by third-party computer forensic experts under our supervision.*

*It is far more cost effective to protect your assets  
and prevent theft in the first place.*

*Look to Bond.*



For more information:



Heath J. Szymczak

*In Buffalo, contact Heath Szymczak*

Heath has extensive litigation experience in business-related torts, complex commercial litigation, and other civil litigation, including, among other areas, contractual disputes, unfair competition claims, shareholder derivative actions, shareholder freeze-out actions, corporate valuation, breach of fiduciary duty claims, class action consumer litigation, commercial lease disputes, intellectual property disputes, healthcare network provider disputes, replevin actions, construction litigation, estates litigation, lien enforcement, products liability defense, personal injury defense, insurance fraud, and insurance coverage disputes.

Avant Building - Suite 900, 200 Delaware Avenue, Buffalo NY 14202-2107  
716.416.7057; hszymczak@bsk.com



Sanjeeve K. DeSoyza

*In Albany, contact Sanjeeve DeSoyza*

Sanjeeve is a labor and employment law attorney who represents private and public sector clients before federal and state courts and various government agencies in employment discrimination, wage and hour matters, unfair competition and contract disputes. He also has extensive experience in collective bargaining negotiations, labor arbitrations, proceedings before the National Labor Relations Board and management of daily labor relations issues.

22 Corporate Woods Boulevard, Suite 501, Albany, NY 12211-2503  
518.533.3206; sdesoyza@bsk.com



Howard M. Miller

*In Garden City, contact Howard Miller*

Howard is a labor and employment law attorney whose practice includes most aspects of employment and education law and related litigation. Many of his cases have received media attention and have been reported in the New York Law Journal and Employment Law 360. Howard frequently lectures on topics such as Constitutional Law, non-compete and trade secret litigation, employment and Constitutional issues relating to social networking sites and various aspects of employment discrimination and education law.

1010 Franklin Avenue, Suite 200, Garden City NY 11530-2900  
516.267.6318; hmiller@bsk.com



James D. Dati

*In Naples, contact James Dati*

Jim is a valued partner and trusted advisor to owner-executives, decision-makers, high net-worth individuals and others needing help with business and real estate legal matters. His objective is to deliver to Bond clients unfaltering legal advice, counsel and high-quality work product. Jim achieves this by fully understanding each client's goals, expectations, values and concerns, gathering and processing relevant information, identifying possible decision options and finally implementing the client's directives. For many clients, Jim serves as their "Outside, In-House Counsel" due to his sagacity, judgment and broad experience with many divergent legal issues.

4001 Tamiami Trail North, Suite 250, Naples FL 34103-3555  
239.659.3845; jdati@bsk.com



David E. Prager

*In New York City, contact David Prager*

David helps employers avoid costly employment disputes when they can be circumvented, and face down those in which a challenge is inevitable. Skilled in negotiation, dispute resolution and arbitration, employers turn to David with their labor and employment issues, starting with counseling and dispute-avoidance, through successful litigation and closure.

600 Third Avenue, 22nd Floor, New York, NY 10016-1915  
646.253.2330; dprager@bsk.com



Bart Chacchia

*In Rochester, contact Bart Chacchia*

Bart leads the business law practice in Bond's Rochester office and advises a wide spectrum of clients, including entrepreneurs, closely-held businesses, venture-backed companies, private equity funds and their portfolio companies, banks, financial institutions, private lenders, publicly-traded companies and public utilities, in connection with business entity formation and capitalization; incentive plans, executive compensation and employment agreements; customized domestic and international contracts; intellectual property protection; growth plans and commercial synergies; banking and finance; regulatory affairs and compliance; mergers and acquisitions; restructurings, reorganizations and consolidations; business succession planning and exit strategies; and ownership disputes and derivative actions.

350 Linden Oaks, Suite 310, Rochester, NY 14625-2825  
585.362.4742; bchacchia@bsk.com



Louis Orbach

*In Syracuse, contact Louis Orbach*

Lou is deputy chair of the firm's litigation department. He has tried cases to jury and bench, argued appeals, arbitrated and mediated disputes and counseled clients in high stakes matters of contention across New York State and around the country for over 20 years. Lou has proven himself an effective advocate in numerous and diverse venues, from rural county courthouses to the Second Circuit in Manhattan, and in subject areas ranging from civil rights to creditors' rights, intellectual property to employment law and ERISA, and business and commercial law to Title IX.

One Lincoln Center, Syracuse NY 13202-1355  
315.218.8633; lorbach@bsk.com



Commitment • Service • Value • Our Bond

About Bond, Schoeneck & King

Bond, Schoeneck & King PLLC serves individuals, companies and public-sector entities in a broad range of areas. With 265 lawyers, we represent clients in financial services; manufacturing; agribusiness; commercial lending and real estate development and construction; energy; health care and long term care; and municipalities, school districts, higher education, and other exempt and nonprofit organizations. We maintain nine offices across New York; one in Naples, Florida; and one in Overland Park, Kansas. Bond is committed to understanding our clients' needs and providing comprehensive, practical, high-quality and responsive solutions. We strive to maintain the highest professional and ethical standards, and to provide leadership in community activities, pro-bono work and service to the Bar.

Bond, Schoeneck & King PLLC (Bond, we, or us), has prepared this communication to present only general information. This is not intended as legal advice, nor should you consider it as such. You should not act, or decline to act, based upon the contents. While we try to make sure that the information is complete and accurate, laws can change quickly. You should always formally engage a lawyer of your choosing before taking actions which have legal consequences. For information about our firm, practice areas and attorneys, visit our website, [www.bsk.com](http://www.bsk.com). Prior results do not guarantee a similar outcome.