MANAGING BLOGS, INSTANT MESSAGING, AND PHONES WITH CAMERAS IN ORDER TO AVOID THE LOSS OF TRADE SECRETS

Hospitality Law Seminar - Eastern Region

June 1-2, 2009
Baltimore, Maryland

J. Scott Humphrey
Michael D. Wexler
Seyfarth Shaw LLP
131 South Dearborn Street, Suite 2400
Chicago, Illinois 60603
(312) 460-5000
shumphrey@seyfarth.com
mwexler@seyfarth.com

SEYFARTH SHAW LLP
ATTORNEYS

J. Scott Humphrey

Mr. Humphrey is a partner in Seyfarth Shaw's Trade Secrets, Restrictive Covenants and Corporate Espionage Group. He serves on the Group's National Steering Committee and has successfully prosecuted and defended trade secrets and restrictive covenant cases throughout the United States for clients in the technology, securities and financial services, transportation, electronics, software, hospitality, medical, insurance, healthcare, consumer products, and manufacturing industries. Scott has also led trade secret audits for both public and privately held corporations, and is a contributing author to "Trading Secrets," a legal industry blog that monitors and discussed trade secrets, restrictive covenants and computer fraud issues.

Michael D. Wexler

Mr. Wexler is a partner in the firm's Chicago office and National Chair of the Firm's Trade Secrets, Restrictive Covenants and Corporate Espionage Group. His practice focuses on trial work and counseling in the areas of trade secrets and restrictive covenants, corporate espionage, unfair competition, complex commercial disputes, intellectual property infringement and white collar criminal defense. A former state prosecutor, Mr. Wexler's extensive investigatory experience and considerable jury trial practice enables him to advise clients with regard to potential disputes and represent clients through and including a determination of their rights at trial. Mr. Wexler has successfully obtained and defended temporary restraining orders and preliminary and permanent injunctions in several jurisdictions. He has represented clients in the insurance, securities, finance, banking, transportation, manufacturing, technology, pharmaceuticals, advertising, real estate, employment, medical equipment and computer industries throughout the United States.

Table of Contents

I. INTRODUCTION – SCOPE OF ARTICLE

In today's business climate of advancing technologies and a sagging economy, the possibility of losing trade secrets through computers and other electronic data devices is greater than ever. Simply put, the proliferation of computers, e-mail, voice-mail, intranets and the Internet have changed the methods and requirements for storing and communicating trade secrets and other confidential information, as well as increased the likelihood of innocent and intentional trade secret disclosure.

The use of external storage devices, such as personal data assistants (PDAs), portable hard drives, Palm Pilots, Blackberries, and even cell phones, makes protecting confidential information even more complicated because these devices can easily send sensitive company data and trade secrets to a competitor or public forums such as blogs and industry web sites. Hence, past practices of keeping hard copies of confidential documents and information under lock and key are no longer sufficient protection against the misappropriation of trade secrets, and companies that do not have adequate safeguards are vulnerable to the loss of critical data. Similarly, companies that do not act swiftly when responding to trade secret misappropriation risk losing their competitive advantage to not only competitors, but to the public as well.

Consequently, companies need to develop and review security measures designed to protect trade secrets. In doing so, companies must understand how a court determines what merits trade secret protection and whether a company has taken adequate measures to protect trade secrets. Such measures include not only traditional protection methods, such as keeping documents under lock and key, but also measures designed to prevent disclosure in today's digital age. Accordingly, this article reviews what constitutes a trade secret under the law and reasonable measures that enable a court to invoke trade secret protection. This article then discusses additional steps companies should consider implementing in order to combat trade secret disclosure through electronic media devices and forums (such as blogs and cell phones), and remedies available to a company once trade secret misappropriation occurs.

II. TRADE SECRET LAWS

In order to appropriately protect trade secrets, a company must first understand how the courts decide what is a "trade secret" and what types of confidential information have been afforded trade secret protection.

A. Restatement (First) of Torts – Definition of Trade Secret

Published in 1939, the Restatement Section 757, Comment (b) 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". *Restatement (First) of Torts*, § 757 (1939).[1] The Restatement also lists the following six factors courts should consider when determining whether information is, in fact, a trade secret:

---

[1] In addition, the Restatement (Third) of Unfair Competition (released in 1995) defines a trade secret as "any information that can be used in the operation of a business or other enterprise and

- The extent to which the information is known outside of the business;
- The extent to which the information is known by employees and others involved in the business;
- The extent of measures taken to guard the secrecy of information;
- The value of the information to the owner and the owner's competitors;
- The amount of effort or money expended by the owner in developing the information; and
- The ease or difficulty with which the information could be properly acquired or duplicated. *Id.*

B. The Uniform Trade Secrets Act

The Uniform Trade Secrets Act ("UTSA") was approved by the National Conference of Commissioners on Uniform State Laws in 1979 and amended in 1985. The differences between the Restatement and the UTSA are that the UTSA does not require that the trade secret be in use to be protected, and the UTSA also explicitly protects negative information about research or a process that does not work. The UTSA has become the seminal authority for trade secrets law and Forty-six states, as well as the District of Columbia, have adopted the UTSA into their own statutory codes. (Massachusetts, New Jersey, New York, and Texas have not adopted the UTSA and rely either on their own statutory schemes or common law to protect trade secrets).[2]

1. UTSA's Definition of a Trade Secret

According to the UTSA, a trade secret is:

> information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being

---

that is sufficiently valuable and secret to afford an actual or potential economic advantage over others." *Restatement (Third) of Unfair Competition*, § 39 (1995).

[2] *See* Ala. Code § 8-27-1; Alaska Stat. § 45.50.940; Ariz. Rev. Stat. § 44-401; Ark. Cod § 4-75-601; Cal. Civ. Code § 3426.1; Colo. Rev. Stat. § 7-74-101; Conn. Gen. Stats § 35-50; Del. Code tit. 6, § 2001; D.C. Code § 48-501; Fla. Stat. §688.001; Ga. Code § 10-1-761; Haw. Rev. Stat. § 482B-1; Idaho Code § 48-801; 765 Ill. Comp. Stat. §1065/1; Ind. Code §24-2-3-1; Iowa Code § 550.1; Kan. Stat. § 60-3320; Ky. Rev. Stat. § 365-880; La. Rev. Stat. § 1431; Me. Rev. Stat. § 1541; Md. Code § 11-1201; Mich. Comp. Stat. § 445.1901; Minn. Stat. § 325C.01; Miss. Code § 75-26-1; Mo. Rev. Stat. $417.450; Mont. Code § 30-14-401; Neb. Rev. Stat. § 87-501; Nev. Rev. Stat. § 600A.010; N.H. Rev. Stat. § 350-B:1; N.M. Stat. § 57-3A-1; N.C. Gen. Stat. § 66-152; N.D. Cent. Code § 47-25.1; Ohio Rev. Code § 1333.61; Okla. Stat. tit. 78 § 85; Or. Rev. Stat. § 646.461; 12 Pa. Cons. Stat. § 5301; R.I. Gen. Laws § 6-41-1; S.C. Code § 39-8-10; S.D. Codified Laws § 37-29-1; Tenn. Code § 47-25-1701; Utah Code § 13-24-1; 9 Vt. Stat. § 4601; Va. Code § 59.1-336; Wash. Rev. Code § 19.108.010; W. Va. Code § 47-22-1; Wis. Stat. § 134.90; Wyo. Stat. Ann. § 40-24-101).

generally known to, and not being readily ascertainable by proper means by, other person 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.

2. Examples of Trade Secrets

As a result of the trade secret definition put forth by the UTSA, Restatement (Third) of Unfair Competition, and state common law, a wide variety of information can be afforded trade secret protection so long as the information provides actual or potential economic value from its secrecy and the company takes/implements measures that are reasonable under the circumstances to maintain the information's secrecy. *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 997, 104 S.Ct. 2862, 2872 (1984) ("if an individual discloses his trade secrets to others who are under no obligation to protect the confidentiality of the information, or otherwise publicly discloses the secrets, his property right is extinguished"). If the above requirements are met, courts have found the following information to qualify as a "trade secret" under the UTSA and/or applicable state law:

- Customer lists. *New England Ins. Agency, Inc. v. Miller*, 1991 WL 756666 (Conn. Supr. Ct. 1991); *Merger Ventures, Inc. v. Barnak*, 1990 WL 172048 (Del. Ch. Nov. 2, 1990); *Dickeman Assocs., Inc. v. Tiverton Bottled Gas Co.*, 594 F.Supp. 30, 35 (D. Mass. 1984); *National Employment Sarv. Corp. v. Olsten Staffing Serv., Inc.*, 761 A. 2d 401, 404-05 (N.H. 2000); *Merrill Lynch, Pierce, Fenner, Smith, Inc. v. Dunn*, 191 F.Supp.2d 1346, 1351 (M.D. Fla. 2002); *Dicks v. Jensen*, 172 Vt. 43, 708 A.2d 1275 (2001); *Brisken v. All Seasons Servs.*, 615 N.Y.S. 2d 166, 167 (4th Dep't 1994) (customer lists qualify as trade secrets if the employer can establish that the lists are treated and protected as confidential information); *Mettler-Toledo, Inc. v. Acker*, 908 F.Supp. 240, 247 (M.D. Pa. 1995) (a customer list can be a trade secret so long as the list cannot be easily or readily obtained from an independent source).[3]

- Customer databases as well as internal information concerning knowledge of customers' buying habits, markup structure, merchandising plans, sales projections and product strategies. *U.S. Land Services, Inc. v. U.S. Surveyor, Inc.*, 826 N.E.2d 49 (Ind. Ct. App. 1st Dist. 2006) (the database was given trade secret

[3] *But also see Brett Senior & Assocs. P.C. v. Fitzgerald*, 2007 U.S. Dist. LEXIS 50833 (E.D. Pa. July 13, 2007) (a client list was not a trade secret under Pennsylvania law because the list was available from other sources); *ENV Servs. Inc. v. Alesia*, 2005 NY Slip Op 51947U (N.Y. Sup. Ct. 2005) (trade secret protection for a client list not available because the names and addresses on the list were readily ascertainable through sources outside the business such as the internet); *Marietta Corporation v. Fairhurst*, 301 A.D.2d 734, 754 N.Y.S.2d 62 (3rd Dep't 2003) (Hospitality amenities supplier's pricing data, marketing strategies, and customer lists were not given trade secret protection because the supplier failed to provide evidence demonstrating how each item was kept "a secret").

protection, even though some customer information was available over the Internet or other public sources, because plaintiff took adequate measures to keep the *entire* contents of the database confidential); *Platinum Mgmt., Inc. v. Dahms*, 666 A.2d 1028, 1038 (N.J. Super. Ct. Law Div. 1995); *Benode Aluminum of Florida, Inc. v. Rodriguez*, 712 So.2d 438, 439 (Fla. 3rd Dist. Ct. App. 1995).

- Documentation concerning knowledge and methods of operations, as well as confidential information concerning the "modus operondi" of the company. *United Rug Auctioneers, Inc. v. Arsalen*, 2003 WL 21527345 (Mass. Sup. Ct. 2003); *Roto-Die, Inc. v. Lesser*, 889 F.Sup. 1515, 1518 (W.D. Va. 1995).

- Marketing and sales information. *Radisson Hotels International, Inc. v. Westin Hotel Company*, 931 F.Supp. 638 (D. Minn. 1996)(Hotel franchisor's marketing information concerning travel agent incentive program could constitute "trade secrets" under Minnesota Trade Secrets Act).

- Business plans, as well as a company's financing plan, marketing strategies, future plans and methods for training and development. *Eastern Artificial Insemination Coop. v. La Bare*, 619 N.Y.S.2d 858 (3rd Dep't 1994); *Elm City Cheese Co. v. Federico*, 251 Conn. 59, 72 A.2d 1037 (1999).

- Scientific data such as chemical processes and manufacturing methods. *Del Monte Fresh Product Co. v. Dole*, 136 F.Supp.2d 1271, 1292 (S.D. Fla. 2001); *Penalty Kick Mgmt. Ltd. v. Coca-Cola*, 164 F.Supp.2d 1376, 1380 (N.D. Ga. 2001); *North Carolina Farm P'ship, L.L.C. v. Pig Improvement Co.*, 163 N.C. App. 318, 593 S.E.2d 126 (2004).

- Cost and pricing information. *LeJeune v. Coin Accepters, Inc.*, 381 MD 288, 849 A.2d 451 (2004).

III. IMPLEMENTING REASONABLE EFFORTS TO PRESERVE SECRECY

A. General Comments

Although there is no bright line rule, companies need to make sure that they are taking reasonable efforts to keep confidential/trade secret information "confidential" in order to achieve trade secret protection under the law. *Ruckelshaus*, 467 U.S. at 997; *BDT Products, Inc. v. Lexmark, International, Inc.*, 274 F.Supp.2d 880, 891 (E.D. Ky. 2003)("It is axiomatic that without secrecy, no trade secret can exist"). Although what efforts are considered "reasonable" will vary with the circumstances, it can generally be said that an employer will need to show that it has a policy for maintaining the secrecy of confidential information and restricting access to such information in order to receive trade secret protection under the law. The policy typically includes:

- Measures to physically secure documents containing trade secret information and establishing repositories for trade secret information;

- Restricting access to trade secrets to a "need to know" basis;

- Clearly labeling documents and other repositories as containing trade secrets; and
- Implementing a policy for document protection, retention, and destruction, including provisions for marking confidential documents.

The policy should be clearly communicated to employees, preferably as part of the employee handbook and as part of any nondisclosure covenant signed upon hiring. Put another way, employer policies and manuals should cover the use of trade secrets/confidential information. In doing so, the policies and manuals need to instruct and inform the employee to keep trade secret information a secret. Best practices would require the employee to read the policy and then acknowledge that he/she understands and will abide by the policy. Similarly, restrictive covenant agreements should also contain provisions stating that the employee understands that he/she will be provided trade secret information and is not authorized to disclose this information to anyone not authorized to receive it, either during or after their employment.

In addition, companies should also consider:

- Providing specific written notice to employees (in addition to the Employee Handbook) who receive trade secrets that the information is in fact a trade secret and is not to be disclosed or used by the employee for any unauthorized purpose.
- Issuing confidentiality and non-disclosure agreements to employees and third parties who have access to the trade secrets.
- Establishing and periodically monitoring/revising confidentiality policies that are distributed to all employees.
- To the extent necessary/possible, separate components of a trade secret between or among departments and/or company personnel.
- If outside vendors will possess or review confidential information, establishing secrecy agreements with the vendors.
- Implementing sign in/sign out procedures for accessing and returning trade secret information.
- Reproducing only a limited number of trade secret documents, and installing procedures for collecting all copies after use.
- Restricting physical access to facilities to visitors by requiring visitors to sign in at a receptionist desk and be escorted by an employee.
- Using magnetic card entrance restrictions.
- Placing labels on confidential information.

- Implementing an employee awareness program with periodic reminders regarding the handling of confidential information.

- Conducting periodic security audits to determine whether confidentiality procedures are being followed.

- Instituting authorized codes or passwords for access to copying machines and computers.

- Conducting formal exit interviews with departing employees in order to remind the former employees of their continuing obligations with respect to confidential information and to ensure that all confidential information has in fact been returned to the company.

B. Trade Secrets Audit

Companies should also consider conducting a "trade secrets audit" in addition to the traditional methods discussed in Section III (A). The audit would include reviewing how the company defines trade secret material, what information falls under that definition, what information that may previously have been treated as a secret no longer needs protection, who has access to the trade secret (and who should have access to the trade secret), and the procedures and channels in place to maintain secrecy. Conducting regular audits can determine exactly how the trade secret(s) is kept, establish whether the procedures in place for keeping the trade secret "a secret" are actually being followed, and find gaps in protection before misappropriation occurs. The audit also encourages the company to develop better methods for protecting the trade secrets secrecy. It is best if the audit is conducted by a cross-functional team consisting of personnel from human resources, information technology, and legal departments, as well as outside counsel.

C. Additional protection measures for the digital age

Today's trade secrets are kept not only under lock and key but also on computer databases and other electronic media devices; and courts have held that such storage does not negate trade secret protection so long as companies take reasonable efforts to preserve the secrecy of the "trade secret" being preserved on a computer or electronic device. *Softell, Inc. v. Dragon Med. & Scientific Communications, Inc.*, 891 F.Supp. 935, 946 (S.D.N.Y. 1995); *Blue Cross & Blue Shield of Connecticut Inc. v. Dimartino*, 1991 WL 127094 (Conn. Super. Ct. 1991); *Hilb, Rogal & Hamilton Co. of Atlanta Inc. v. Holley*, 284 Ga.App. 591 (2007) (customer contact information retained on a personal electronic organizer may constitute a trade secret under Georgia law if necessary security measures are in place).[4] Moreover, the ease of electronic transmission of sensitive data - through the Internet, camera phones, blackberries,

[4]It should also be pointed out that a computer program, by itself, can constitute a trade secret so long as it is protected as a trade secret. *Liberty Am. Ins. Group, Inc. v. West Point Underwriters L.L.C.*, 199 F.Supp.2d 1271, 1302 (M.D. Fla. 2001); *CMAX/Cleveland, Inc. v. UCR, Inc.*, 804 F.Supp. 337, 357 (M.D. Ga. 1992).

PDAs, etc… - makes it particularly important that adequate security measures are in place to protect company secrets that are kept in electronic form.

1. General steps

In addition to the items discussed in Sections III (A) and (B), companies must have in place computer and communications systems policies that are distributed to all employees. E-mail policies alone are no longer sufficient to protect a company's confidential information. New technologies, such as instant messaging, stand-alone storage drives, external email accounts and electronic organizers need to be accounted for in computer and communications policies. These policies should be incorporated into the employee handbook and discuss how confidential information should be used and handled.

In addition, employees that handle confidential/trade secret information through electronic devices should be required to review all policies that concern the use of confidential information and acknowledge that they will abide by the policies. Verification pages, demonstrating that the employee received and reviewed the employee handbook, as well as all confidential/trade secret polices, should be kept in the employee's personnel file. Companies should also consider:

- Encrypting and/or password protecting confidential information stored on computers or other electronic media devices. (And changing passwords on a periodic basis).
- Employing multi-layered passwords for trade secrets and confidential information.
- Limiting physical and computer access to trade secrets and confidential information on a need-to-know basis.
- Not using the Internet to transmit proprietary information or using encryption software to transmit the confidential information.

2. Blogging protections

The Internet, with its blogs, industry websites, and chat rooms, has become a fertile ground for the destruction of trade secrets. Simply put, a disgruntled employee can place trade secrets on a blog or in a chat room and, within seconds, the trade secrets can be accessed by millions of people located throughout the world. Accordingly, companies need to be vigilant in not only protecting their trade secrets but also with respect to monitoring and, to the extent possible, maintaining their employees' ability to disclose trade secret information in a public forum. Companies should also consider the potential ramifications of hosting blogs and chat rooms that allow third parties to post comments and information. As is discussed later, the UTSA allows for injunctive relief and damages against companies that knew (or had reason to know) that received information was a trade secret and should not have been disclosed to them. Thus, although little case law currently exists, it is not unreasonable to envision a scenario where a company that hosts a blog is brought into litigation between a competitor and its former

employee who published the former employer's confidential information on the blog. Accordingly, with respect to blogs and chat rooms, companies should:

- Have an internal policy outlining what can and cannot be placed on the blog. Any employee who chooses to participate in the blog should acknowledge the policy before posting any blog article or information. In general terms, the policy should cover not only the disclosure of confidential and proprietary information, but also what is and is not acceptable blog content.

- Assign a senior management level employee to be responsible for reviewing blog content before posting.

- Institute a monitoring policy in order to make sure that neither the company's, nor anyone else's, trade secret information is being posted on the blog, as well as a policy that allows the company to quickly remove any confidential information that is posted on the blog.

- Publish a disclaimer on the blog site regarding the statements, positions and opinions placed on the blog.

If outside parties are allowed to post on the blog, then the company should require the outside party to acknowledge that they will not distribute or disclose any confidential or trade secret information. The blog should also issue a disclaimer stating that individuals or entities may post articles or comments to articles on the blog, but that these comments or articles are not the express views of the company and that the company is not responsible for the posting of confidential information.[5]

3. Electronic Media devices

All laptops, computers, cell phones, blackberries and other PDAs used by employees should be company owned. In addition, the company should inform all employees, through a written policy contained in the Employee Handbook, that these items are company property, should only be used to conduct company business, and that violating a company policy can result in immediate discharge. In addition, companies should also explain that there is no privacy expectation with respect to these devices, and that all company devices are subject to company inspection at any time and must be returned upon request or at the time of termination.

Obviously, only a minimal number of companies take all of the measures or precautions listed above and the key thing to remember is that the law does not require absolute secrecy. Rather the relevant standard is whether reasonable steps were taken to protect the trade secrets

[5] Please note that these recommendations only concern the disclosure of trade secret information and should not be considered a substitute for other disclaimers and/or policies concerning blog use.

secrecy. As such, companies should understand that protecting trade secrets is not a "one size fits all" approach, and consider the above items when discussing the implementation of trade secret protection measures. After such consideration, a company can then tailor the relevant items into a program that makes sense from both a business and legal perspective.

IV. MISAPPROPRIATION

Even the most diligent companies, with the most developed protection measures, can be the subject of trade secret misappropriation. Hence, companies need to be aware of the rights and remedies available to them when trade secret misappropriation occurs, as well as the need to act quickly in order to protect the trade secrets "secrecy" and disclosure to non-authorized individuals and entities.

A. Legal Protections and Remedies

Once information qualifies as a "trade secret," the UTSA will protect it from misappropriation. "Misappropriation" is the *use or disclosure* of the information without consent of the owner under one of the following circumstances:

- The individual acquired the information by *improper means*. "Improper means" includes theft, bribery, misrepresentation, breach of a duty to maintain secrecy, espionage, and the like.

- The individual acquired the information from someone else and knew (or had reason to believe) that the person who provided the information either acquired it by improper means or had a duty to maintain its secrecy. Generally, nondisclosure agreements are sufficient to create a duty on the part of the employee to preserve the secrecy of the information.

- The individual knew (or had reason to know) that the information was a trade secret, and that it was disclosed by accident or mistake.

Under the UTSA, a party may seek an injunction for either actual or threatened misappropriation. In addition to granting the injunction, courts may order affirmative acts, such as the return of confidential documents and property. The UTSA also allows a party to recover damages caused by the misappropriation and punitive damages in the event that the misappropriation was willful and malicious. Willful and malicious misappropriation also allows a court to award reasonable attorneys' fees.

In addition to the UTSA, several other statutes may be available to a victim of trade secret misappropriation. For example, the Computer Fraud and Abuse Act (18 U.S.C. § 1030 *et seq.*) ("CFAA") provides a private right of action for injunctive relief and damages against anyone, including former employees and competitors, who intentionally access a computer without authority or exceed their authorization and thereby obtain information from any protected computer involved in interstate commerce. The CFAA also allows for relief against individuals or entities that access a computer without authority and in order to defraud or cause damage. Similarly, the Economic Espionage Act of 1996 (18 U.S.C. §§ 1831-1839) criminalizes the theft or attempted theft of commercial trade secrets and conspiracies to steal such trade

secrets; and the Racketeer-Influence and Corrupt Organizations Act (18 U.S.C. § 1961 *et seq.*) ("RICO") can apply to a trade secrets case when there is an ongoing pattern of conduct that violates certain federal criminal laws, such as mail and wire fraud statutes. RICO imposes *treble* damages and allows for the recovery of attorneys' fees against the offending party, and is not dischargeable in a bankruptcy proceeding.

Finally, certain common law actions may be available to a victim of trade secret misappropriation. Specifically, claims for tortious interference with contract and prospective economic advantage may exist if a third party (i.e., a competitor or former employee) uses trade secrets to interfere with an ongoing relationship, so long as there is a reasonable expectation that the relationship will continue. A company may also have a breach of fiduciary duty claim against the former employee who misappropriated the trade secret.

B. Trade Secret Litigation – *Starwood v. Hilton*

Finally, one of the highest profile lawsuits of 2009 demonstrates the exposure a Hospitality company faces when its trade secrets are allegedly misappropriated by a competitor. On April 16, 2009, Starwood Hotels & Resorts Worldwide, Inc. ("Starwood") filed a Complaint in the United States District Court for the Southern District of New York against Hilton Hotels Corporation ("Hilton") and two former Starwood executives who are now Hilton's Global Head of Luxury & Lifestyle Brands and Global Head of Luxury & Lifestyle Brand Development, respectively. *Starwood Hotels & Resorts Worldwide, Inc., v. Hilton Hotels Corporation et al.*, 09 CV 3862 (S.D.N.Y. April 16, 2009). In the Complaint, Starwood alleges that Hilton hired the two former employees in order to develop a competing luxury brand for Hilton, known as "Denizen." The former employees, who were Starwood's former President and Senior Vice President of Starwood's Luxury Brands Group (a Group that includes such well recognized brands as the St. Regis and W Hotels), were bound by a confidentiality agreement with Starwood that prohibited the disclosure of Starwood's confidential trade secret information.

According to Starwood's Complaint, the two former employees took over 100,000 documents containing Starwood's most competitively sensitive trade secret information when they left Starwood for Hilton. The confidential trade secret information included Starwood's strategic plan for its luxury hotel brands. The two former employees allegedly accomplished their theft by emailing files to personal accounts, downloading files and information to personal USB drives and other portable electronic storage devices, bringing in a personal laptop and downloading confidential information into the laptop, using DVDs and other electronic media devices to download confidential information, and shipping materials directly to Hilton's offices. Starwood claims that Hilton then used this confidential trade secret information to develop its own competing luxury brand, Denizen.

Starwood's nine count Complaint includes claims against the former employees for breach of their confidentiality agreements, a tortious interference claim against Hilton for alleged interference with Starwood's contractual relationship with the two former employees, misappropriation of trade secrets claims against both the former employees and Hilton, and additional claims of unfair competition, theft/conversion, and violation of the Computer Fraud and Abuse Act. After the Complaint was filed, the parties entered an agreed order for a preliminary injunction that placed the entire Hilton Denizen team on paid administrative leave of

absence and suspended all further development of the Denizen Hotels brand. *Starwood,* 09 CV 3862 (S.D.N.Y. April 23, 2009). The preliminary injunction also ordered Hilton and the two former employees to return all Starwood confidential trade secret information to Starwood. Moreover, the U.S. Attorney's Office for the Southern District of New York opened an investigation into Starwood's claims and Hilton received a grand jury subpoena requesting documents, including documents relating to Starwood's confidential information, on April 20, 2009. Tamara Audi, *U.S. Probes Allegations About Hilton*, The Wall Street Journal, April 21, 2009.

Thus, *Starwood v. Hilton*, is a strong reminder of why companies need to take significant measures to protect their trade secrets, as well as a solid example of the actions and remedies available to the victims of trade secret misappropriation. Accordingly, companies need to remain vigilant with their trade secret protection measures, especially when a company's trade secrets and confidential information can be passed to a competitor or the public in the blink of an eye.