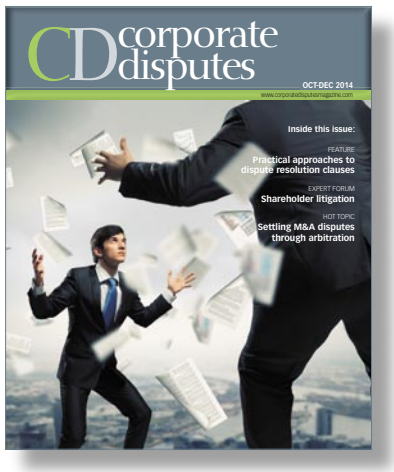
REPRINT

CD corporate disputes

TRADE SECRET DISPUTES AND EMPLOYMENT RISKS

REPRINTED FROM:
CORPORATE DISPUTES MAGAZINE
OCT-DEC 2014 ISSUE



www.corporatedisputesmagazine.com

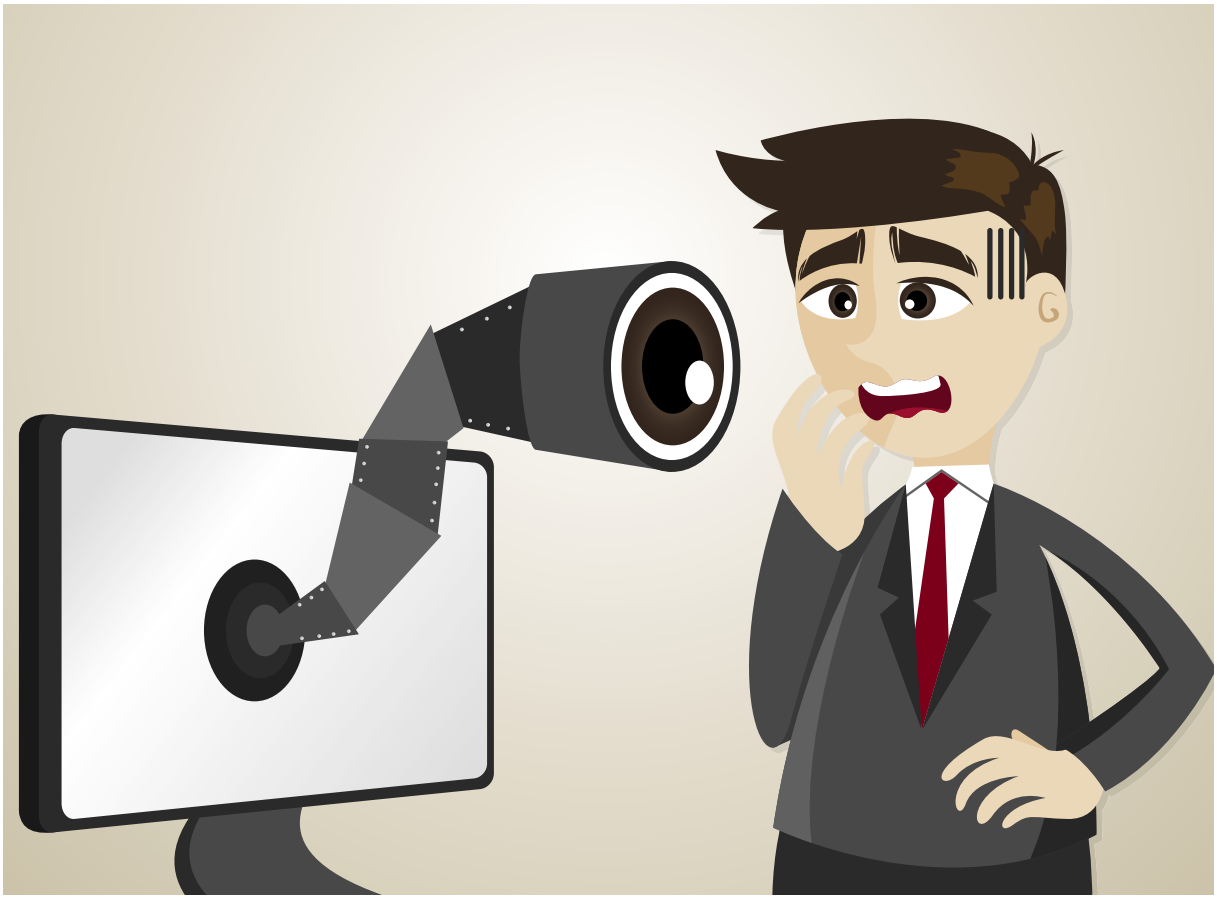
Visit the website to request
a free copy of the full e-magazine

SEYFARTH SHAW

Published by Financier Worldwide Ltd
corporatedisputes@financierworldwide.com

MINI-ROUNDTABLE

TRADE SECRET DISPUTES AND EMPLOYMENT RISKS



PANEL EXPERTS

Robert B. Milligan
Partner
Seyfarth Shaw LLP
T: +1 (310) 201 1579
E: rmilligan@seyfarth.com

Robert B. Milligan is a partner in the Litigation and Labor & Employment Departments of Seyfarth Shaw LLP. Mr Milligan co-chairs the firm's Trade Secrets, Computer Fraud & Non-Competes practice group. His practice encompasses a wide variety of commercial litigation and employment matters, including general business and contract disputes, unfair competition, trade secret misappropriation and other intellectual property theft, franchise litigation, real estate litigation, insurance bad faith, invasion of privacy, consumer and employee class actions, wrongful termination, discrimination and harassment claims, wage and hour disputes, ADA and OSHA compliance, whistleblower and SOX cases, bankruptcy and other business torts.

Michael D. Wexler
Partner
Seyfarth Shaw LLP
T: +1 (312) 460 5559
E: mwexler@seyfarth.com

Michael D. Wexler is a partner in the firm's Chicago office and chair of the national Trade Secrets, Computer Fraud and Non-Competes Practice Group. His practice focuses on trial work and counselling in the areas of trade secrets and restrictive covenants, corporate espionage, unfair competition, complex commercial disputes, intellectual property infringement and white-collar criminal defence in both federal and state courts. 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.

CD: Could you provide a brief snapshot of current trends in trade secret disputes? Do companies need to be more aware of the potential risks in this area?

Milligan: Data theft of valuable company trade secrets through the use of portable electronic storage devices is occurring more and more, as is theft through cloud storage. We are also seeing an increase in more sophisticated hacking of company networks to obtain proprietary data by organised crime and foreign companies or states. Technological tools and employee use of personal mobile devices such as smartphones and tablets have given rise to a parallel trend of employers allowing – or requiring – their employees to use their own personal mobile devices at work. This 'Bring Your Own Device' (BYOD) movement can provide benefits to employees and employers, such as convenience, greater flexibility and productivity, as well as cost savings. However, BYOD programs can also create risks for employers. Companies need to be aware of potential data security issues, BYOD policies in a unionised workforce, employee privacy concerns and intellectual property issues. Moreover, the recovery of stolen information and workplace investigations can be hampered by employee-owned devices, not to mention challenges in litigation when trying to gain access to such devices where privacy considerations are often leveraged. Additionally, attacks on reasonable secrecy measures – part of the definition of a trade secret – is also on the rise: one court recently ruled that password protection alone was not enough to demonstrate reasonable secrecy measures.

Wexler: Further, like the EU, the United States is considering enhancing trade secret protections through additions to its laws. There are two bills pending in the United States Congress to create a civil cause of action for trade secret misappropriation in federal court. If passed, the legislation would provide companies with an additional forum and remedy to combat trade secret theft. With the increasing accessibility of data from a variety of electronic devices and threats by insiders and outsiders, companies also need to be more aware of potential risks to their data and ensure that they have appropriate policies and agreements in place with employees, vendors and business partners, as well as top of the class data security protections.

CD: How severe is the threat of losing trade secrets to a departing employee or departing executive? What are some of the common scenarios in which trade secrets can be compromised in this manner? Does the threat level change depending on the size of the company – small cap, mid cap, Fortune 50?

Wexler: The threat of losing trade secrets to a departing employee is real and not a matter of if, but when. Prudent companies will make sure that they have appropriate processes in place to address the threat when it occurs. As today's businesses meet the challenges of intensifying global competition, a more volatile workforce and information being transmitted at an unprecedented speed, they also face a greater risk of losing their valuable proprietary information to theft, inadvertent disclosure or coordinated employee departures. At a minimum, failure to take both proactive and immediate reactive measures could result in significant loss of profitability and erosion of an established employee and customer base. The threat of losing trade secrets to a departing employee or executive is enhanced if you don't have appropriate policies and agreements in place to prevent such theft or hold employees accountable for their unlawful conduct. And it can happen so easily and rapidly: one thumb drive can carry millions of pages of proprietary information and company information transferred to a personal email account or in a personal cloud all pose means for theft.

Milligan: Just look at recent headlines involving some of the world's largest companies who have seen their proprietary information compromised by insiders and outsiders. The crown jewels of many companies are at risk, and millions of dollars are in play. Lack of market secrecy measures, sloppy practices including poor supply side protections, lack of employee education and stale agreements and policies, poor security and different standards for executives who say one thing and do another are all common scenarios that put a company at risk. Common scenarios in which trade secrets can be compromised include letting an employee take company data when he or she leaves. Another red flag scenario is not utilising non-compete or non-disclosure agreements. There can also be scenarios where the particular industry is highly competitive and competitors are willing to take the enhanced risks to acquire the business or technology. In such scenarios, companies need to make sure they have in place appropriate onboarding and off-boarding practices and procedures, and use the appropriate agreements so they are not exposed. In our experience, the threat level does not necessarily change depending on the size of the company, but the magnitude of harm may increase. The larger the company, the more information to protect and the more employees and third parties to regulate and police. But small and mid-cap companies have similar concerns because they oftentimes have innovative technology that competitors or other third parties want, so these companies can also be vulnerable.

CD: What steps can companies take during the hiring process to reduce the threat that it may later be sued for trade

secret misappropriation – particularly executives or those employees with higher level access to sensitive IP assets?

Milligan: Companies need to have a thoughtful, proactive process in place when hiring employees from competitors that is calculated to ensure that new employees do not violate their lawful agreements with their former employers, including using or disclosing their former employers' trade secrets, and retaining any of their former employers' property. It is important to regulate who interviews the job candidate and evaluate the candidate's non-compete or confidentiality agreement. Advise company personnel who are interviewing the candidate not to ask about a competitor's confidential information during the hiring process. Focus the interview on the recruit's general skills and experience in the industry. It's also important not to disclose company trade secrets to the candidate – be careful of the access permitted to the candidate. Candidates for employment should sign certifications that they will not disclose any trade secrets of their current employer. Additionally, make sure you analyse a recruit's agreements in advance of an offer being made. Should the candidate accept an offer, provide clear instructions to the employee that you don't want the former employer's trade secrets or property and use agreements with the employee documenting the same. There are unique issues surrounding the retention and departure of high-level executives, particularly related to non-compete and trade secret issues. Since businesses can become targets of trade secret-related lawsuits if they hire executives and senior management who have worked at a competitor and misappropriate trade secrets or otherwise violate their restrictive covenants, it's important for companies to conduct due diligence on prospective employees and make sure that they have thoughtful plan in place before bringing on any high risk hires.

> **"Exposure of confidential company information and employee privacy rights are all issues that companies are now struggling with."**
>
> *Robert B. Milligan, Seyfarth Shaw LLP*

Wexler: Simple steps such as retaining hard drives when an employee leaves and inspecting computers, devices, cloud storage, and email

accounts can alert an employer to theft of information. More sophisticated methods such as forensic exam and monitoring software can also detect theft. Most of all, create a culture in which recruits and new employees are told 'we do not want anything from your prior employer'. Some additional best practice considerations follow below. Do not allow a recruit to do any work for your company until he or she has left his or her prior employer. Assist the employee in announcing the change in employment upon commencement of employment as appropriate. Focus on making the transition as smooth as possible for the current employer and encourage the departing employee to give proper notice and work out a mutually agreeable transition schedule with his or her current employer. With respect to the employee's new position, don't put the employee in a position in the company where he or she will necessarily need to reveal trade secrets. Finally, HR personnel needs to follow up with the employee to make sure that she is following her agreements and not pushing the envelope, and also follow up with managers to make sure the employee is doing the same.

CD: In what ways is the technology now available to employees changing the playing field in terms of loss or theft of trade secrets?

Milligan: The constant evolution of technology, particularly in mobile devices, data storage and security, and social media, has created legal challenges for companies and the playing field has changed tremendously. Portable electronic storage devices, online data storage and personal email are available to employees for nominal to no expense and can provide the means to trade secret theft. Additionally, business leaders often want data and information immediately and often want to make it accessible to various constituents, but companies don't necessarily keep up with the latest security in protecting such data. Companies need to stay on top of technology, including the latest in data storage and security and storage devices. Hacking of computers and mobile devices is more of a concern these days, and more mobility for employees also means more potential security issues for companies. Companies also need to stay on top of social media. Given its rapid and somewhat haphazard growth, social media carries with it a set of issues that traditional avenues of trade secret disclosure do not. For instance, unlike the departing employee who knowingly takes with him a box of documents, the relaxed and non-professional environment of social media sites could lead to employees disclosing confidential information without even realising they are doing so. Exposure of confidential company information and employee privacy rights are all issues that companies are now struggling with.

Wexler: Social media privacy legislation has become increasingly common in the United States and often impacts trade secret investigations. Issues related to social media privacy in the workplace are not going away and we expect to see more disputes to define acceptable practices in this area. In light of this uncertainty, employers should determine whether their company has employees in any of the states that have adopted or are planning to adopt social media privacy laws in order to ensure compliance with such laws. Employers should also be aware that state laws may restrict requests for information about such activity. Counsel should review the applicable state social media access law before asking an employee for any account-related information. Additionally, employers should not overlook social media evidence in conducting employee investigations, and trade secrets and restrictive covenant lawsuits, but make sure that their company's review and access of such information does not violate applicable law.

CD: How can companies avoid trade secret misappropriation and what should they do if they suspect misappropriation has occurred? What forensic investigation options might be available?

Wexler: Apart from civil liability, the Economic Espionage Act makes it a federal crime to steal trade secrets, and companies can be liable if they hire employees who misappropriate trade secrets for their new employers' benefit. Make sure your executives know the importance of playing by the rules. Employers can best avoid trade secret misappropriation with solid hiring practices and strong off-boarding procedures which are calculated to protect trade secrets and honour lawful agreements, coupled with effective ongoing employee training on trade secret protection and fair competition. Protecting your company information is critical to avoid trade secret misappropriation, and companies should work with their outside counsel to create solid policies and agreements, and solutions for onboarding to avoid exposure on restrictive covenants and trade secrets. It's also crucial to know your business partners, and have them vetted, so that they don't expose your valuable trade secrets. Critical to any trade secret matter is the thorough investigation of what, if any, wrongdoing occurred. Companies should work with legal counsel who is experienced in conducting such investigations. Comprehensive interviews and a review of relevant files, emails and workspaces are often the starting points of a competent investigation.

Milligan: We also regularly collaborate with forensic experts and computer specialists to find out how secrets were taken, and by whom, and to preserve any evidence necessary to future litigation. It is important to preserve data, review emails and talk to relevant witnesses to interpret the forensic

data. A digital forensics examination often includes collecting and analysing artefacts from the operating system, internet history, and unallocated space. Routine e-discovery does not typically delve into questions about the source computer or storage device and ESI, although e-discovery may uncover the need to ask questions related to internet history, webmail, cloud storage, mobile devices and phone back-ups, and removable devices.

CD: How should companies interact with criminal prosecutors and federal/state law enforcement to complement civil claims for trade secret misappropriation?

Milligan: Private companies can investigate misappropriation claims and provide information to authorities for purposes of prosecuting Economic Espionage Act or Computer Fraud & Abuse Act claims as well as similar state criminal laws, but businesses need to be aware of two important points. First, allowing law enforcement access to the business can be a double edged sword creating interference with operations and disclosure of more information than the business may want. Second, when conducting an investigation, be certain to follow accepted forensic practices and chains of custody in collecting information. In sum, ensure that you have your house in order so you don't become the target of an investigation. When considering criminal prosecutions, always be cognizant of the ethical rule required of attorneys that generally prohibits threatening or initiating criminal proceedings to gain an advantage in a civil proceeding. Consultation with criminal authorities should be done in secrecy and ideally by non-attorneys so as not to run afoul of ethical rules. However, note an attorney can have contact with authorities; it is not prohibited in and of itself.

Wexler: It should also be noted that criminal prosecutors may make a request regarding the secrecy of the investigation or to hold off taking certain actions in the civil matter – or pursing the case altogether while the criminal case is ongoing – as they are focused on the criminal matter whereas a company and its counsel may be focused on the civil matter and damages. These differing interests can collide at times, so coordination is key. No private right of action exists yet under the Economic Espionage Act. The US Senate and House are currently considering legislation on this issue.

CD: What kinds of challenges do US companies face in pursuing trade secrets and non-compete claims against foreign companies, particularly from China?

Milligan: US companies may face the challenge of not being able to enforce injunctive relief orders and judgments, as well as jurisdictional challenges posed by foreign companies. Additionally, in some

cases, Chinese companies doing business in the US have quite limited assets in the US and individual defendants may be judgment proof. Even if a US company obtains a favourable judgment from the US court, the judgment may not be recognised or enforceable in China, and thus, the company may not obtain sufficient monetary or equitable remedy. Therefore, the US company must carefully select its business partners and the jurisdiction in a confidentiality or non-compete agreement to attempt to enhance its ability to obtain an injunction and judgment. If forced to sue abroad, remember the court systems are different and there are different views on IP. Your company may not be able to get complete relief in a foreign jurisdiction. The EU Commission has proposed a directive to harmonise trade secrets law in Europe that may assist in this regard in the future if approved.

CD: What are some practical considerations for US companies or multinational companies doing business in Asia and Europe to protect their trade secrets and confidential information?

Wexler: Know your business partners. Have them fully vetted so they don't steal your IP. Try to protect your supply side with appropriate agreements. You should also be careful about what you share with your business partners. If it is bet-the-company information, consider keeping that internal. In addition to getting employees and business partners to execute well-prepared agreements, training – both on-board and on-the-job – can be a powerful measure. Employers should make sure that access to trade secrets and confidential information is granted only to those with necessity to know and make sure your local workforce abroad is trained on company policies and signs appropriate agreements to protect IP. Also consider local variations. Realise that you are not in the US, and the legal systems and respect for IP may be different. For example, in China, different locales may have different views on trade secret protections and non-compete agreements. For instance, the statutory minimum non-compete compensation in Shenzhen is higher than the one in Shanghai. US companies or multinational companies doing business in China should be aware of such local variations and may need to take different measures in different places to ensure protection.

Milligan: Within a foreign forum the selection of the right venue, meaning a locale where the court is more willing to implement the rule of law, is essential. In China, for example, the enforcement varies by locale. For instance, recent decisions indicate that Shanghai courts are more willing to give protection to the employer in trade secret and non-compete cases, including issuing injunctive relief. Try to use contractual choice of law, consent to jurisdiction, and forum clauses for the most

favourable forum for you. Also consider international arbitration. Assess your security vulnerabilities, particularly in light of the foreign locale, and put in place appropriate safeguards. Carefully access your IT security in foreign countries and be alert for unauthorised monitoring and surveillance. Provide training to executives on travelling abroad and conducting business abroad to ensure that trade secrets are not carelessly compromised.

CD: In your experience, what should a company do if a trade secret dispute arises between it and a former employee?

Milligan: If a company suspects that valuable information has been improperly taken or compromised, you need to first assess the potential competitive threat to the company. It's important to take fast, effective action and consider whether to pursue civil remedies or criminal intervention against the former employee. If litigation is anticipated with the departure of an employee, take precautionary steps immediately. Secure and establish a chain of custody for all items returned by the departing employee, including laptop computer, desktop computer, USB devices, tablets and physical property. Secure and maintain a chain of custody of the employee's office and the items in that office until it is searched. Retain outside counsel to investigate the departure and have outside counsel secure the services of a digital forensic investigation firm with a good reputation. If the employee is computer savvy, do an immediate search of the internet for relevant materials posted to social media sites, including LinkedIn, Facebook and Twitter.

> **"Know your business partners. Have them fully vetted so they don't steal your IP. Try to protect your supply side with appropriate agreements."**
>
> *Michael D. Wexler, Seyfarth Shaw LLP*

Wexler: When our clients are faced with possible trade secret misappropriation by former employees, we immediately investigate and develop the facts through interviews, document review and collaborate with a qualified digital forensic expert. Forensic investigation of computing devices to identify the possible theft of confidential information is a must. We assess the company's business objectives as well as the chance of success, and assuming that there is sufficient evidence to pursue,

we demand compliance and appropriate remedies via cease and desist demands prior to the initiation of litigation. Should written requests for compliance not be successful, we seek injunctive relief and damages to protect company assets and further our client's objectives.

CD: In the battle against trade secret theft and related disputes, do companies place enough importance on the language and provisions contained in employment contracts? How can employment contracts be strengthened to either reduce trade secret theft or improve the company's chances of reaching a successful outcome in a trade secret dispute?

Wexler: In our experience, companies should place more importance on their agreements with employees, vendors and business partners to protect trade secrets. Companies need to strengthen the language and provisions contained in such agreements, including clearer definitions of protectable trade secrets, return of company property provisions, appropriate restrictive covenants and appropriate forum and choice of law provisions. Well-drafted agreements can reduce the risk of information being misappropriated. Such agreements should be updated annually, as needed, based on changes in the law, and companies should routinely audit their practices to make sure each employee has an appropriate agreement. Companies should also make it an agreed requirement for employees to sit for an exit interview and return any company confidential information stored on any personal devices. Finally, agreements should include an attorneys' fee provision for breach.

Milligan: Additionally, a thorough exit interview should be conducted at the time any employee separates, and as part of that exit interview process, each exiting employee should be given a written reminder of their ongoing trade secret, confidentiality and social networking obligations, and should be asked to sign the reminder acknowledging receipt and their agreement to comply with such obligations. The exit interview is also the time to get company property returned by the departing employee and make any arrangements for the return and remediation of company property on any personal devices. CD

EDITORIAL PARTNER

Seyfarth Shaw

www.seyfarth.com

At **Seyfarth Shaw**, we are leading the way to deliver legal services more effectively, more efficiently, more transparently. Seyfarth Shaw LLP provides thoughtful, strategic, practical legal counsel to client companies and legal teams of all sizes. With more than 800 attorneys in the US, London, Shanghai, Melbourne and Sydney, we offer a national platform and an international gateway to serve your changing business and legal needs in litigation, employment, corporate, real estate and employee benefits. Seyfarth's Trade Secrets lawyers work to help clients prevent trade secret theft or misappropriation, violations of non-competes and computer fraud, and if necessary, pursue aggressive litigation tactics to stop the further spread or use of information and other improper activities.

KEY CONTACTS

Robert B. Milligan
Partner
Los Angeles, CA, US
T: +1 (310) 201 1579
E: rmilligan@seyfarth.com

Michael D. Wexler
Partner
Chicago, IL, US
T: +1 (312) 460 5559
E: mwexler@seyfarth.com