Morgan Lewis | White Paper

REDUCING YOUR COMPANY'S EXPOSURE TO TRADE SECRET LITIGATION WHEN KEY EMPLOYEES COME AND GO

October 2015

www.morganlewis.com

THE NIGHTMARE SCENARIO

Within the span of two weeks, Mr. Smith and Mr. Wilson, two top managers from your $2 billion corporation, resign. Both managers had complete, unfettered access to your corporation's trade secrets and confidential information, including pricing and staffing formulas, clients' requests for proposals, and bid information.

One month earlier, Mr. Smith and Mr. Wilson incorporated a competitor company with a covert business partner. In the time leading up to their resignations, the managers purchased new cell phones and set up new email addresses in the competitor business's name, and used hard drives and flash drives to extract documents from your corporation's computers. Up until the time they resigned, Mr. Smith and Mr. Wilson sent emails from your corporation's servers to their covert business partner that contained confidential information about your key clients.

Through your own forensic investigation, you learn that the managers downloaded and transferred thousands of your corporation's documents from the external devices straight to the competitor company's computer system. In fact, you even uncover an email from Mr. Smith to Mr. Wilson sent the day before his resignation, stating, "I trashed everything on my computer since I have to turn it in tomorrow."

Could this have been prevented? What now?

KEEP YOUR EYES ON THE PRIZE WHEN A KEY EMPLOYEE DEPARTS

Don't add insult to injury

When a key employee announces that he or she is leaving, it can wreak havoc on the business. Maintaining clients, ensuring coverage, managing investor relations—all of these things come into play with immediate urgency. The inconvenience of an employee departure can turn into a serious problem that requires an enormous outlay of resources if misappropriation of confidential information becomes an issue.

Simply having noncompete agreements with key employees is no longer enough. To avoid making a bad situation worse, there are a few steps to take immediately when a key employee departs, as well as day-to-day best practices that should be integrated into your business and its policies.

Day-to-Day Best Practices

1. Know what's in the vault.

The first thing that corporate counsel must do to protect against disclosure of confidential information is to clearly identify what types of information are confidential or proprietary. A vague or ambiguous policy will not do—only where it is clear that certain information is to be treated as confidential will protections be sufficient. That said, not everything can be marked confidential. The protection "loses its teeth" when a company uses the designation loosely, marking everything from YouTube videos to takeout menus as "confidential." While it may require some resources to ensure that confidential information is designated and maintained appropriately, it is a wise investment to ensure the protection of that information.

It is also important to identify who has access to the various types of confidential information so that you know who the "key players" are. The day an employee leaves the company is not the time to learn that he or she had access to proprietary or confidential trade secrets that could easily have been taken before departure.

2. Develop a detailed policy.

There is no such thing as an effective "one-size-fits-all" confidentiality/trade secret protection policy. Each company has unique assets and resources, and requirements and restrictions. If your company does not already have a policy regarding intellectual property (IP), work product, confidential information, or trade secret protection, it is vital that you develop such a policy. In the event that an employee subverts the policy and provides trade secrets to a new employer, that well-defined and strictly managed policy can make all the difference in enforcing a later action for misappropriation. In the current legal regime, the employer is required to demonstrate that it took appropriate steps to protect its confidential information, including enforcing policy protocols.

At minimum, a sound policy on confidential information should include

- the company's **expectations** for its employees regarding confidential information, including a prohibition on unauthorized copying or disclosure;
- a **definition** of what is considered confidential or proprietary, including as many specific types of information as possible;
- the **consequences** to the employee for violations of the policy, and the rights of the employer in the event of a violation;
- the employee's **responsibility** to return all company technology and confidential information before leaving employment;
- a mechanism for ensuring that employees receive the policy and sign an **acknowledgment** of their responsibilities under the policy; and
- continuous **training** of key employees on a regular basis as part of the company's compliance program.

3. Establish security protocols.

A well-drafted and publicized policy will do little if it is not enforced with certain day-to-day security safeguards. Appropriate security measures must include limits on access to confidential information in all forms. Locks on file cabinets are no longer enough in the digital world. For example, password requirements for accessing or sharing certain types of information are now widely employed. It is critical that employers understand how to limit access to databases and other information repositories, and ensure that there are systems in place that can track who can access, modify, or delete information. This is important not only for protection, but also for enforcement. For example, to succeed in an action against a former employee for violation of the Computer Fraud and Abuse Act (CFAA)[1] or the Stored Communications Act (SCA),[2] an employer must demonstrate that the employee exceeded his authorization to the electronic information at issue.[3] Having clear protocols in place may make it easier to

[1] 18 U.S.C. § 1030.

[2] 18 U.S.C. § 2701.

[3] *See Penrose Computer MarketGroup, Inc. v. Camin*, 682 F. Supp. 2d 202, 210-12 (N.D.N.Y. 2010) (where district court denied motion to dismiss CFAA and SCA claims based on allegations that the employee accessed his manager's email account and obtained proprietary information, but dismissed SCA claims based on allegation that the employee deleted his own work email). There is a split among the circuits regarding the application of CFAA, but the weight of authority has been shifting against the broad interpretation that an employee's downloading and adverse use of information that he or she is authorized to access violates the CFAA. *See Dresser-Rand Co. v. Jones*, 957 F. Supp. 2d 610 (E.D. Pa. 2013) (in which the district court granted summary judgment on a CFAA claim based on the allegation that two employees downloaded their employer's proprietary information for use by a competitor prior to resigning because the information was validly accessed). The key to proving a CFAA claim under these circumstances may be a well-drafted policy on confidential information coupled with a noncompetition agreement.

show that certain access was unauthorized and exceeded the employee's authority. A skilled IT department manager or outside consultant will be able to assist in identifying appropriate security practices.

Another protective tool is to embed identifiers or tags for highly confidential or sensitive information that will appear on any electronic or printed copy of the material. This makes clear to anyone in possession of the material that the information is confidential and proprietary property of the company.

Further, counsel must understand the company's electronically stored information (ESI) storage and destruction policies. In addition to concerns about unintentional spoliation of evidence based on automatic deletion or overwrites, be mindful of how data or information could be intentionally destroyed. For example, ensure that employees are not able to download software that can "wipe" or overwrite the memory of their company-owned laptops.[4] Understand the extent of your company's ability to investigate whether data has been deleted, copied, removed, or transmitted. In the event of a security breach, where immediate action may be needed, you should not need to "get up to speed" on what your internal systems can do—you should already know. Finally, understand the resources available to you within your organization so that you will know when it is appropriate to recommend the retention of a forensic investigation or retrieval expert.

4. Enforce compliance.

Robust confidentiality and security policies mean nothing if they are not followed. IT departments can perform certain forensic reviews relatively easily and regularly. However, it is also wise to consider a more robust periodic audit—including an occasional forensic audit—to determine to what extent any policies are being violated or are otherwise ineffective.

Similarly, periodic reminders of the policy and what information is considered confidential or proprietary are important. In-person training sessions or online webinars can be effective and also allow an employer to ensure that each employee has participated. Simply handing a copy of the policy to a new employee is not enough. In the event of litigation, the company must have a compelling story to tell about the proactive steps it has taken to protect its confidential information. Think about ways to communicate the message that will be effective for your organization and also persuasive to a judge if you have to defend your company's process later.

It is also important that protective practices be enforced at all levels of the company. Consistent application of IP and confidentiality policies will act as a deterrent and help, in the event of litigation, to show that the company has taken reasonable steps to secure confidential information. While all of these steps may require a financial investment, proactive attention to these issues can protect the company's most valuable assets, and will make it easier to enforce confidentiality agreements down the line.

Take Immediate Steps When a Key Employee Departs

Now that you've gotten your house in order, what do you do when you learn that a key employee is leaving? How do you ensure that no vital information "walks out the door"? It is entirely possible that an outgoing employee may take confidential information without even knowing it. For example, what if your key employee loads photographs of his kids that are stored on his work computer to a portable flash drive and inadvertently copies confidential company files in the process?

---

[4] In a recent Utah case discussed *infra*, employees downloaded software with the ability to "wipe" or permanently delete files from their laptops in an attempt to conceal their misappropriation of their former employer's confidential information. The IT expert retained by the plaintiff discovered the fraud and was able to show that the file names of the destroyed documents were likely highly relevant to the litigation. As a sanction for these and other transgressions, default judgment was entered against the defendant with an award of attorneys' fees to the plaintiff. *Philips Elec. N. Am. Corp. v. BC Technical*, 773 F. Supp. 2d 1149, 1158-59 (D. Utah 2011).

Having a well-established exit protocol for key employees will help prepare everyone for the transition. Here is a list of steps to consider as part of such a protocol:

- Establish an exit interview team (Exit Team) that is familiar with the employee's work, projects, and external relationships.
- The Exit Team should include (1) HR personnel responsible for the employee, (2) a business head to whom the departing employee reports and does work, (3) an IT representative, (4) a member of the company's legal department, and (5) company personnel familiar with the employee's outside business relationships and connections.
- The Exit Team should develop questions and specific protocols for the departing employee's exit process. Counsel should review the questions and protocols.
- Immediately restrict access to certain files and set a date certain for the departing employee's return of computer equipment, mobile devices, and security badges.
- Consider engaging the IT or security department in an analysis of whether the employee copied, transmitted, or destroyed key information prior to the submission of his or her resignation notice.
- Provide a written copy of the confidential information policy to the employee and name individuals whom the employee can contact to go over any questions about the policy.
- Schedule a pre-exit interview to remind the employee about the confidentiality policies and to go over the company's expectations with respect to confidential information and ESI. A representative from HR and IT or security should be present. (*See* SIDEBAR below).
- During the interview, give explicit instructions not to copy, send, download, or transmit information of any kind outside of the company; ask the employee to sign an acknowledgment of receipt of both the policy and the request not to transmit information.
- Follow up the interview with a letter reminding the employee of these responsibilities. Ensure that this letter is given to all departing employees prior to departure.
- Request that the employee work with the IT department to retrieve any personal, nonconfidential information from company computers and explicitly instruct the employee *not* to download, email, or transmit materials without explicit permission and assistance from IT. For example, even if the employee only wants to download photos of his kids or similar files from his computer, make sure he understands that he should not perform any copying, modifying, or destruction of files without involving IT.
- On the employee's last day, ask him to again sign an acknowledgment that he has followed the applicable protocols.
- Consider sending a letter to the employee's new employer confirming the steps your company took to protect its confidential information and your former employee's obligations with respect to confidential information.

SIDEBAR: Pre–Exit Interview Questions

Briefing employees on confidentiality expectations before they depart can prevent problems down the road. Do not wait until the employee's last day—speak with the employee as soon as possible after you learn that he or she is leaving.

Below are some questions or points to consider including in your pre–exit interview:

- Do you have any company or proprietary information in files (electronic or hard copy) at home?

- Have you used your home or other personal computer for company work?
- Do you use your personal mobile device (smartphone or tablet) for work?
- Have you used a flash/USB drive for work purposes, whether it was a personal flash/USB drive or one provided by the company?
- Have you downloaded or otherwise transmitted documents to any of your personal email, social media, or other accounts? Why?
- Does anyone else have access to your electronic work files and accounts?
- Do you understand that you must work with the IT department to return all company information from any source, including your home accounts? This also includes retrieving personal information from company systems; we will help you do this properly so that you do not inadvertently violate the policy.
- Do not copy, alter, download, or delete files without conferring with IT. You may violate your obligations as an employee if you do so.
- Have you upheld the confidentiality policy and do you agree to continue to do so?
- Has anyone asked you to violate the policy or to otherwise obtain confidential information for that person's benefit? Remember that if you are solicited to provide confidential information to anyone, your duty as an employee is to inform the company immediately.

Best practices for exit interviews such as those described above may help your company protect against disclosure of confidential information, as well as prevent litigation headaches down the road. Remember that the best prevention is a clear message regarding your policy, repeated often, and consistently enforced.

AVOIDING A TROJAN HORSE: BEST PRACTICES WHEN HIRING KEY EMPLOYEES

The Honeymoon Is Over

Your company is thrilled to have wooed a key employee who can add value. Even if you've determined that there are no noncompete issues, your job does not end there. A new employee who brings confidential or proprietary information from his former employer can expose your company to liability, even if no one at your organization asked him to do so, or even if the transmission is wholly unintentional. You must take proactive steps during the hiring process to ensure that confidential or proprietary information from a competitor does not end up in your company's possession and thereby exposing it to serious expense and liability.

For example, in a recent Utah case, a default judgment was entered against the defendant company in a misappropriation of trade secrets matter after it was discovered not only that employees (who had left their employment with the plaintiff to join the defendant) brought over the plaintiff's confidential information with them, but also that the defendant company's executives destroyed those files despite litigation hold protocols, and that the executives subsequently lied under oath about the destruction.[5] While this nightmare for counsel is an extreme example, all companies must take proactive steps to ensure that new employees do not bring along a "Trojan horse" of competitor information that would expose them to liability.

[5] *Philips Elec. N. Am. Corp.*, 773 F. Supp. 2d at 1158-59. The case was also referred to the United States Attorney's Office for investigation of alleged perjury.

This threat is not just one where the specter of damages looms if a case for misappropriation is made or where an injunction could be issued; real expenses may be incurred before the employee even starts his employment. When a company must search its information management systems to prove that no confidential information has been brought over by a new employee, it can easily cost tens of thousands of dollars.

Protective Policies

Having explicit company policies in place—such as those that prohibit the solicitation or dissemination of other companies' confidential or proprietary information—can help save the day. Including language within the confidential information policy regarding employees' legal and ethical obligations with respect to competitors' information will demonstrate that the company is not interested in acquiring secret information through unauthorized means.

Similarly, it should become standard practice to inform incoming employees of this policy. Waiting until an employee starts work may be too late. During employment negotiations (sensitive though they may be), it is important to clearly communicate that the company is not interested in acquiring the confidential information of the potential employee's current employer. Sending a letter to this effect during final negotiations is one step that can demonstrate the company's good-faith efforts to prevent acquiring competitors' information. The letter should include a reminder that the employee must work with his current IT department to gather any personal information, and confirm that any information he takes with him is approved by the employer.

If the incoming employee will be subject to an employment agreement, consider including a clause in the incoming employee's agreement making a violation of the policy grounds for termination of the agreement by the employer. An indemnification clause protecting the employer from gross violations of the agreement may also be considered, although its enforceability may depend on the circumstances surrounding any violation.

Awareness and Training

The new employee should be reminded of this portion of the confidential information policy during the orientation and training process. Consider having representatives of the legal and IT departments meet with the employee to explain and reiterate the policy, and to obtain an acknowledgment of the policy from the employee.

Additionally, preventive measures may be worth considering. Confer with your IT department to develop a protocol for discovery and quarantine in the event that the company becomes aware of a possible issue with a competitor's confidential data. Having a well-planned protocol in place will save you valuable time. Further, ensure that as part of your IT department's regular review of the efficacy of its confidential information protections, the department is also ensuring that competitors' information has not found its way into the system. In addition, create a means for employees to report possible violations of the policies to underscore the seriousness of the policies. Make sure that employees know whom they can contact in the event that they believe there may have been a violation. Having such policies in place can limit an employer's vicarious exposure to liability.

Documentation

Documentation of the company's efforts to ensure that it has not improperly acquired others' confidential information is crucial. Trainings must be well documented, with records of the attendees and what written copies of relevant policies were provided to participants. Documentation of all efforts to prevent incoming employees from transmitting confidential data must also be created contemporaneously. Self-serving deposition testimony that "we told him not to do that" will rarely be compelling after the fact. Similarly, merely having a policy will be ineffective if new employees are not made aware of it in a timely

manner, and if current employees are not reminded of their continued obligations not to solicit or acquire competitors' confidential information, and to report possible violations of the policy.

DISPUTE STRATEGY: DUTIES FOR MAINTAINING AND PRESERVING ELECTRONIC DATA WHEN AN ISSUE ARISES

What You Need to Know When a Situation Arises

Of course, sometimes even the best prevention strategy is not enough. What happens if you discover that a former employee has copied sensitive files, or if you are served with a cease-and-desist letter from a competitor after a new hire comes on board? In the event of litigation concerning confidential or trade secret information, counsel must be able to show that it took immediate action to preserve relevant information. But what do those duties entail, and when do they arise? It might be more complicated than you think.

As soon as the company is aware of possible litigation, an effective litigation hold must be issued. Simply telling employees not to destroy files will not be enough. As with any litigation, a hold must be descriptive of the information necessary to retain and must be distributed to the appropriate individuals. As the potential issue evolves, be sure to revisit the litigation hold often and update it as new information becomes available. Redistribute the hold periodically to remind employees of their continued duties.

Similarly, determine what preservation steps can be reasonably taken with your IT department to preserve server information, backup tapes, or other company data. In most instances, an individual's computers or email accounts are implicated, so consider having IT "image" hard drives or mobile devices as soon as possible. As a practical matter, you need to confer with the IT department to determine what sort of notice will be provided to employees that their hard drives or other devices will be searched. If you believe there may be any chance that an employee could attempt to deliberately destroy data, take steps to understand what, if any, intentional destruction could actually be affected by the employee, as well as ways you can prevent it. All of these steps should be well documented by in-house and outside counsel as part of the litigation preparation process, and counsel must take steps to protect the work-product privilege.

Consider whether it may be advantageous to send a letter to the other side that reiterates your company's efforts to protect confidential information and states that your company has taken steps to prevent competitors' information from being obtained by its employees or potential employees. Also, consider whether to offer to cooperate with the competitor to identify any potentially confidential information in your possession and to quarantine such information if discovered. Cooperation at the beginning may prevent escalation of the issues, but also may be futile if the other side is determined to engage in litigation.

While a process of disseminating litigation holds and preserving information at the first inclination of potential litigation is not without expense and effort, early preservation efforts may prevent the company from being taxed with fees or costs based on spoliation issues.

Obligations to Preserve

Although the need to preserve information is obvious, it is not always clear when that duty actually arises and what types of information must be preserved. Again, there is no "one-size-fits-all" answer to the question of what must be preserved, since it depends heavily on the factual circumstances surrounding the case and the type of information that was allegedly misappropriated. The good news is that preservation efforts do not have to be Herculean to be effective; rather, they must be reasonable and proportional.

Courts have provided some guidance on when the duty to preserve arises in different situations. For example, in a case involving an employee who left his former employer to work for a competitor, the former employer's duty to preserve information that could have provided possible defenses to a misappropriation claim was triggered when the former employer reasonably anticipated litigation. However, the former employer did not engage in spoliation where, at the time it anticipated litigation, it was not aware that others in the organization had possibly gained the competitor's information, and therefore the former employer was not responsible for preserving all files for those individuals at that time.[6] In that case, the duty to preserve information for those individuals arose once the former employer learned that they may have had relevant files, but by that time some files had been destroyed. The fact that files were not preserved was not sufficient to warrant spoliation sanctions. It's important to note that the former employer's demonstrated policy against misappropriation of information and its reminders to employees of their legal and ethical obligations with respect to competitive intelligence helped swayed the court against an adverse inference that information that was lost was probative of the issues in the case.[7]

On the other hand, when is a potential defendant "on notice" that ESI must be preserved? Courts have found that when an action is filed, a clear duty to preserve is triggered. For example, in an action alleging improper access to a secure dealer server by a former employee now working for a competitor, the competitor was not required to preserve information before the suit was filed, even though the competitor was aware that its employees may have improperly accessed the server. However, once the suit was filed, the duty to preserve was triggered, and the competitor/defendant was responsible for ensuring that a timely effort was made to collect and preserve evidence. Because the defendant waited for three months to even confirm that individuals were aware of (and abiding by) the litigation hold, the court sanctioned the defendant by making it pay for the costs incurred for the forensic examination of the defendant's computers, as well as attorney fees incurred by the plaintiff in bringing the motion to prevent spoliation.[8] The court noted that, "[i]n order to avoid sanctions, such as these, parties must cooperate and voluntarily preserve, search for, and collect ESI."[9]

The Forensic Examination

In cases such as these, the forensic examination and collection processes are paramount. Simply relying on employees to voluntarily disclose information regarding misappropriation is likely to be wholly insufficient. An in-house IT department may be too "close" to the relevant individuals to conduct a truly independent investigation. Counsel must consider whether an independent forensic examination is best. Where a departing employee had extensive access to company trade secrets/confidential information, an independent forensic investigation will be crucial. It is important to note that a forensic examination is not the same as a typical document review. A forensic examination deals with examining ESI systems and history rather than the content of the ESI itself. This is one area where companies might consider seeking to share costs with opposing counsel, because forensic examinations can be expensive. However, it is critical to understand your company's particular situation and systems before making any promises regarding forensic examination. In short: Don't promise what you can't do!

Conducting an independent forensic examination very early in the process may demonstrate that the company's systems do not contain misappropriated information, and may also help to convince the court that the company takes its confidentiality policies and procedures seriously. Even if issues are discovered,

---

[6] *E.I. Du Pont de Nemours & Co. v. Kolon Indus., Inc.*, Case No. 3:09cv58, 2011 WL 1597528, at *13-18 (E.D. Va. April 27, 2011) (denying a motion for sanctions for spoliation of evidence where the court determined that plaintiff had taken reasonable steps to preserve when it became aware of additional possible sources of information).

[7] *Id.* at *18.

[8] *Nacco Materials Handling Grp., Inc. v. Lilly Co.*, Case No. 11-2415, 2011 WL 5986649 (W.D. Tenn. Nov. 16, 2011).

[9] *Id.* at *13.

getting them out in the open at the beginning—rather than after prolonged discovery—can make all the difference in how a case progresses.

Have a Compelling Story

As counsel, you want to be in a position to tell a compelling story to a competitor's counsel, judge, or jury about how your company has made significant efforts to prevent issues relating to misappropriation of information. By clearly defining policies, communicating them effectively and often, and by taking a few additional common-sense precautions, your company may save itself serious litigation headaches. While the investment on the front end may require some justification, it could very well be what saves the day in the end.

Contacts

If you have any questions or would like more information on the issues discussed in this White Paper, please contact any of the following Morgan Lewis lawyers:

Philadelphia

Larry L. Turner	+1.215.963.5017	lturner@morganlewis.com
Alyssa Kovach	+1.215.963.4618	akovach@morganlewis.com

Houston

Ronald E. Manthey	+1.214.466.4111	ron.manthey@morganlewis.com

Los Angeles

Debra L. Fischer	+1.213.680.6418	debra.fischer@morganlewis.com

About Morgan, Lewis & Bockius LLP

Founded in 1873, Morgan Lewis offers 2,000 lawyers—as well as patent agents, benefits advisers, regulatory scientists, and other specialists—in 28 offices across North America, Europe, Asia, and the Middle East. The firm provides comprehensive litigation, corporate, transactional, regulatory, intellectual property, and labor and employment legal services to clients of all sizes—from globally established industry leaders to just-conceived start-ups. For more information about Morgan Lewis or its practices, please visit us online at www.morganlewis.com.