Bloomberg BNA

Daily Labor Report®

NONCOMPETITION AGREEMENTS

Employee turnover is a fact of life, but employers can take a number of measures to minimize the risk that confidential and proprietary information will leave the building with a departing employee, Morgan, Lewis & Bockius attorneys David McManus, Prashanth Jayachandran, and Jason Burns say in this BNA Insights article. They focus on the measures an employer can take before and after learning of an employee's resignation that will help safeguard its prized intellectual assets.

The three attorneys recommend best practices employers can adopt—including executing post-employment agreements, maintaining a strict chain of custody of the employee's electronic devices, and retaining a forensic specialist if necessary—that will help put the employer in the best position possible to take action if an employee's misconduct threatens the employer's competitive advantage.

Are Your Company's Most Valuable Assets and Competitive Advantage at Risk?

BY DAVID A. MCMANUS, PRASHANTH JAYACHANDRAN, AND JASON BURNS

It is a scenario not unfamiliar to employers everywhere that rely upon superior technology and customer intelligence to survive in an increasingly competitive marketplace: without warning, a top salesperson or executive announces his resignation—effective immediately. Invariably, the departing employee is someone in whom the employer has invested significant time and resources, and who has knowledge of—and continues to have access to—the company's most highly sensitive confidential and proprietary information. To make matters worse, the employer comes to learn that the employee intends to join a direct competitor. Under these circumstances, the employer has good reason to suspect that the employee may use its confidential information to gain a competitive advantage while working for a direct competitor.

David McManus (dmcmanus@morganlewis.com), Prashanth Jayachandran (pjayachandran@morganlewis.com), and Jason Burns (jburns@morganlewis.com) are attorneys in the Labor and Employment Practice at Morgan, Lewis & Bockius. McManus is a partner in the firm's New York office, Jayachandran is of counsel in the Princeton office, and Burns is an associate in the New York office.

This article focuses on the measures that an employer can take before and after learning of the employee's resignation that will help safeguard its prized intellectual assets.

First Step: Plan Ahead

The most important steps that an employer can take to limit its potential exposure in situations like the one described will occur well before the employer learns of the employee's departure. In fact, a prudent employer should have in place protective measures from the moment the employee is hired.

First, any employee who may have access to confidential and proprietary information should execute an agreement obligating the employee to safeguard and

 ISSN 0418-2693

protect such information and to return to the employer any and all confidential materials at any time upon the request of the employer and, certainly, at the time of the employee's separation from the company. An effective agreement will broadly delineate categories of confidential/proprietary information, documents, and other materials that the employee must protect, and prohibit the employee from disclosing or otherwise revealing to third parties confidential information without proper authorization.[1]

Second, in a world in which telecommuting is the norm rather than the exception, employees who are permitted to use their own personal electronic devices to access the employer's computing and other internal IT systems should execute a separate agreement concerning the use of the employee's personal electronic devices for any work-related tasks. At minimum, the agreement should (i) require the employee to register any personal devices that the employee wishes to use for company business; (ii) authorize the employer to periodically inspect, both remotely and ''in person,'' any registered devices; and (iii) permit the employer to inspect any registered devices and to delete any company information, and/or documents from the devices upon termination of employment.[2]

Third, the employer should strongly consider requiring employees to execute a noncompete agreement (assuming the employees work in a jurisdiction that permits such agreements), if they are employed in management, sales, research and design, or other positions that present the greatest threat when disclosing or using confidential information with a competitor. The agreement should be drafted by counsel familiar with the enforceability of restrictive covenants under the applicable state law.

Although requirements will vary depending on the jurisdiction, a court is most likely to uphold a carefully tailored covenant that accounts for (i) the employee's specific position, (ii) the scope and nature of the employer's business, and (ii) the potential threat posed by an employee's departure for a competitor. For this reason, employers should regularly review restrictive covenants to ensure that they reflect for each employee the appropriate circumstances of employment.

Any confidentiality or restrictive covenant agreement should specifically acknowledge that a breach of its terms will entitle the company to injunctive relief, a factor that will weigh in the employer's favor should the employer ever seek to enjoin the employee from violating the agreement. See, e.g. *CentiMark Corp. v. Lavine*, No. 11-0757, 2011 BL 196078 (W.D. Pa. July 28, 2011) (granting preliminary injunction in part because employee acknowledged that breach of post-employment obligations would entitle employer to injunctive relief); *Ayco Co., L.P. v. Feldman*, 10-CV-1213, 2010 BL 250395 (N.D.N.Y. Oct. 22, 2010) (evidence of employer's irreparable harm may be found in employee's breach of a post-employment competition provision that provides that the breach will (i) leave the employer without an adequate remedy at law and (ii) entitle the employer to injunctive relief).

Second Step: Take Swift and Immediate Action When an Employee Departs to a Competitor

Responding promptly to news of an employee's departure will mitigate any potential losses or damage that might result from any employee misconduct or foul play. Swift action will also allow an employer to begin building its case in the event legal action becomes necessary to protect the company's confidential and proprietary information.

Any time an employee separates from a company, either voluntarily or involuntarily, the employer should remind the employee, in writing, of his or her obligations under any confidentiality, noncompete, or other applicable agreements. Likewise, the employer should seek from the employee written assurance that he or she has complied with any restrictive covenants.

If the employee has disclosed that he or she is joining a competitor, the employer should consider notifying that competitor, potentially through counsel, of the employee's post-employment contractual obligations. This way, the new employer will be put on notice about the employee's post-employment obligations and may take measures to ensure that the employee complies with these obligations. If the competitor fails to satisfactorily address this matter, taking this step may bolster an employer's ability to obtain injunctive relief, as the employer can demonstrate to a court that the employer's own efforts to resolve the matter were unsuccessful and that judicial intervention is necessary.

It is important that any communications with the employee's new or potential employers be confined to the facts surrounding the employee's departure (e.g., the scope of the employee's obligations under a confidential agreement or the existence of any pending legal action related to the enforcement of that agreement). By keeping the discussion to the ''facts,'' the employer can limit its exposure to potential claims by the employee for defamation or interference with business relations.

If it is not the employer's regular practice to review the email and computing devices of departing employees to ensure that they have not misappropriated any confidential information, the employer should immediately perform a forensic analysis of the computing devices, including any devices subject to a personal computing agreement (e.g., PDAs, smartphones, etc.), of any employee joining a competitor and/or whom the employer suspects may have retained, transferred, or otherwise disclosed confidential and proprietary information.

Similarly, the employer should review any of its internal data systems to determine whether the employee

---

[1] The scope of the information covered under any confidentiality agreement must not be so broad as to potentially interfere with an employee's rights under applicable laws, including Section 7 of the National Labor Relations Act. Section 7 prohibits employers from interfering with employees engaged in certain ''concerted activity'' with respect to the terms and conditions of their employment, which in some circumstances may include employee comments about workplace conditions on social media sites such as Facebook. See, e.g., *Hispanics United of Buffalo, Inc.*, NLRB ALJ, No. 03-CA-027872 (173 DLR AA-1, 9/7/11) (Sept. 2, 2011).

[2] Employers should ensure that any agreement concerning the employee's personal computing devices complies with applicable laws restricting employers' access to information about employees' use of social networking sites. For example, two states, Illinois and Maryland, have recently passed laws that prohibit employers from, among other things, requesting from employees access information related to the employees' social media accounts. A handful of other states are considering similar laws, including Delaware, Massachusetts, Michigan, Minnesota, Missouri, New Jersey, New York, Ohio, South Carolina, and Washington.

  DLR ISSN 0418-2693

has engaged in any unauthorized access or other activity that raises any red flags (e.g., sending company documents to a personal email address or using a USB device to download documents within days of announcing his or her resignation). In any event, the employer should meticulously document the chain of custody of the computing devices for any departing employee in order to bolster the employer's ability to prove that the departing employee was directly responsible for the misconduct and to rebut any potential claims of spoliation.

In addition to potentially uncovering a complete record of any employee misdeeds, a third-party analyst may be a valuable resource for evidence against the employee. See, e.g., *Continental Group, Inc. v. KW Property Management, LLC*, 622 F. Supp. 2d 1357 (S.D. Fla. 2009); *Pharmerica, Inc. v. Arledge*, 8:07-cv-00486-RAL, 2007 BL 234119 (M.D. Fla. Mar. 21, 2007) (relying on evidence gathered from third-party forensic analyst to find that employee had systematically copied and deleted employer's confidential and trade secret information).

Continental Group is instructive on this point. There, the plaintiff's forensic expert testified at length at the preliminary injunction hearing that the employee downloaded voluminous files to her personal laptop and personal portable data storage devices in the days leading up to her resignation. The court specifically acknowledged that it found this testimony credible and ''relied on it extensively'' in compelling the employee to, among other things, return all confidential documents and data to the employer. Thus, promptly retaining a reputable outside expert can be critical to an employer's litigation preparedness and strategy.

Third Step: Initiate Litigation if Necessary

If the employee refuses to fully comply with the employer's demands to return all confidential information or abide by his/her restrictive covenant agreements, the employer may have no choice but to initiate legal action against the former employee and, perhaps, the employee's new employer. In fact, failure to do so may undermine an employer's ability—in subsequent similar claims involving other employees—to demonstrate that the information that it is seeking to protect is ''confidential'' and that the employer will suffer irreparable harm in the event of its disclosure, as described below.

Because of the urgent need to protect confidential information, a temporary restraining order, to be followed by preliminary injunctive relief, will likely be the most expedient method for protecting the employer's business interests.

Although the standard for issuing a preliminary injunction differs depending on the jurisdiction, employers seeking to enjoin a former employee from disclosing confidential information typically must satisfy the test set forth by the U.S. Supreme Court in *Winter v. Natural Resources Defense Council, Inc.*, 555 U.S. 7 (2008): (1) that the employer will suffer irreparable harm in the absence of preliminary relief, (2) that the employer is likely to succeed on the merits, (3) that the balance of equities tips in the employer's favor, and (4) that an injunction is in the public interest. Of course, whether an employer will be entitled to injunctive relief will depend on the individual circumstances surrounding the employee's departure.

In any action for a preliminary injunction, establishing a likelihood of irreparable harm is the single most important prerequisite for obtaining relief from the court. *Faively Transportation Malmo AB v. Wabtec Corp.*, 559 F.3d 110 (2d Cir. 2009). An employer may establish irreparable harm by showing that violation of the employee's post-employment restrictive covenants will result in the loss of client relationships and customer good will that has been built up over time, or in the loss of confidential customer information. See, e.g., *North Atlantic Instruments, Inc. v. Haber*, 188 F.3d 38, 15 IER Cases 731 (2d Circuit 1999); *CentiMark Corp. v. Lavine*, No. 11-0757, 2011 BL 196078 (W.D. Pa. July 28, 2011); *Mintel Int'l Group, Ltd. v. Neergheen*, No. 08-CV-3939, 2008 BL 149547, 27 IER Cases 1876 (N.D. Ill. July 16, 2008); *Johnson Controls, Inc. v. A.P.T. Critical Systems, Inc.*, 323 F. Supp. 2d 525 (S.D.N.Y. 2004). Even where an employee insists that he or she has not misappropriated any confidential customer information, a court is unlikely to credit such testimony where other evidence demonstrates that the employee contacted an employer's customers shortly after his or her departure. See *Ayco Co., LP. v. Frisch*, 795 F. Supp. 2d 193 (N.D.N.Y. 2011).

Courts have also found irreparable harm where a former employer has demonstrated that the disclosure of proprietary information will allow a competitor to ''cut corners'' in the research and development process, thus accelerating the competitor's introduction of a product into the marketplace. See *Universal Engraving, Inc. v. Duarte*, 519 F. Supp. 2d 1140 (D. Kan. 2007) (finding irreparable harm where employee joined competitor to assist in research and design of products similar to those manufactured by former employer). Similarly, an employer can show that it may suffer from unfair competition if an employee familiar with the employer's confidential business and marketing strategies joins a direct competitor. *Nike Inc. v. McCarthy*, 379 F.3d 576, 21 IER Cases 1089 (9th Cir. 2004) (157 DLR AA-1, 8/16/04).

Courts have also found irreparable harm where a former employer has demonstrated that the disclosure of proprietary information will allow a competitor to ''cut corners'' in the research and development process, thus accelerating the competitor's introduction of a product into the marketplace.

In *Nike*, the Ninth Circuit affirmed an injunction enforcing a noncompete agreement against a former Nike executive who resigned from the company to join Reebok. The court found that because the executive had intimate knowledge of Nike's ''product allocation, product development and sales strategies,'' he could develop business and marketing strategies for Reebok that ''could divert a substantial part of Nike's footwear sales to Reebok based on his knowledge of information con-

fidential to Nike,'' even ''without explicitly disclosing this information to any of Reebok's employees.''

When an employee has misappropriated confidential information stored on an employer's computing systems, including email systems, an employer should consider asserting claims under the federal Computer Fraud and Abuse Act (CFAA) or equivalent state laws. Under the CFAA, an employer can bring a claim against a former employee whose unauthorized access of a protected computer results in losses or damages of at least $5,000. 18 U.S.C. § 1030 et seq. In pursuing a CFAA claim, an employer will benefit significantly by demonstrating through forensic analysis the extent of the employee's misconduct. See *Universal Engraving, Inc. v. Duarte*, 519 F. Supp. 2d 1140 (D. Kan. 2007) (finding that results of employer's forensic analysis discredited testimony of former employee who denied accessing his work computer on the dates in question); *Pharmerica, Inc. v. Arledge*, 8:07-cv-00486-RAL, 2007 BL 234119 (M.D. Fla. Mar. 21, 2007) (relying on employer's forensic review of former employee's computer to find likely violation of CFAA).

A benefit of asserting CFAA claims is that an employer may be able to recover certain costs and fees related to the investigation of the employee's misconduct that are not otherwise recoverable under common law absent a contractual agreement with the employee providing for the recovery of such fees. See, e.g., *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 585 (1st Cir. 2001) (holding that a plaintiff may recover under the CFAA costs incurred by hiring a forensic computer consultant to assess and diagnose the extent of a party's unauthorized computer access).

Often, the situation will arise where, prior to separating from the employer, an employee allegedly exceeds his or her computing authority by obtaining for an improper purpose that information which the employee is otherwise permitted to access. Although courts have reached different results in this area, several courts have found that an employer may state a claim under the CFAA when the employee downloads proprietary information for the employee's own benefit or for the benefit of a competitor. See *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582-84 (1st Cir. 2001) (finding that employer was likely to prove unauthorized access under the CFAA where former employee provided proprietary information to new employer in violation of his confidentiality agreement); *Continental Group, Inc. v. KW Property Management, LLC*, 622 F. Supp. 2d 1357 (S.D. Fla. Apr. 2009) (even though employee had access to employer's password-protected files, she exceeded her authority by downloading certain files after she began negotiating to join competitor).

In some circumstances, an employee may exceed authorized access under the CFAA by sending to a personal email address, in the days leading up to resignation, an employer's confidential information regarding its client accounts and marketing strategies. See *Mintel International Group, Ltd. v. Neergheen*, No. 08-CV-3939, 2008 BL 149547, 27 IER Cases 1876 (N.D. Ill. July 16, 2008). Indeed, where the scope of an employee's authorized access is at issue, an employer can bolster its case by showing that the employee did not have a legitimate business reason for accessing or downloading the files in question or that the employee copied or downloaded the information immediately prior to his or her resignation. See *Continental Group, Inc. v. KW Property Management, LLC*, 622 F. Supp. 2d 1357 (S.D. Fla. Apr. 2009); *Mintel Int'l Group, Ltd. v. Neergheen*, No. 08-CV-3939, 2008 BL 149547, 27 IER Cases 1876 (N.D. Ill. July 16, 2008).

An employer may also seek injunctive relief under the CFAA if an employee, in an attempt to ''cover his tracks,'' permanently deletes without authorization the employer's files and emails. *Pharmerica, Inc. v. Arledge*, 8:07-cv-00486-RAL, 2007 BL 234119 (M.D. Fla. Mar. 21, 2007).

Typically, where an employer has satisfied the elements for issuing a preliminary injunction, the court will grant an employer's request that the employee refrain from disclosing, transferring, or otherwise using the confidential information at issue. See, e.g., *Redwood Software, Inc. v. Urbanik*, No. 12-cv-0495, 2012 BL 80632 (N.D.N.Y. Mar. 30, 2012) (Decision and Order); *Universal Engraving, Inc. v. Duarte*, 519 F. Supp. 2d 1140 (D. Kan. 2007); *Hudson Global Resources Holdings, Inc. v. Hill*, No. 07-CV-00132, 2007 BL 190879 (E.D. Pa. May 25, 2007). That said, courts have been reluctant to order employees to turn over personal computing devices for inspection and forensic analysis, particularly where the court has already enjoined the employee from using or disclosing confidential information that might otherwise remain on the employee's personal devices. See *PLC Trenching Co., LLC v. Newton*, No 11-CV-05015, 2011 BL 124067 (N.D.N.Y. May 10, 2011). In *PLC Trenching*, the court found that the forensic investigation requested by the employer was unnecessary given (1) the ethical obligation of the employee's attorney to ensure that his client complied with that part of the court's order enjoining the employee from transferring or otherwise disclosing the employer's confidential information and that (2) if necessary, the employee could seek the information at a later date, for example during the course of discovery.

Accordingly, execution of a ''personal computing agreement,'' as described above, may provide an alternative basis for the court to order a forensic review of non-employer issued computing devices. And a court might be more receptive to ordering an employee to turn over his or her personal devices if the proposed review is to be conducted by an independent, third-party forensic analyst and the employee is given an opportunity to identify and seek protection of objectionable information (such as attorney privileged information) on the devices. See *Ryan, LLC v. Evans*, 8:12-CV-289-T-30TBM (M.D. Fla. Mar. 20, 2012).

Not surprisingly, courts are most likely to compel an employee to produce for review forensic copies of personal computing devices in those cases where the employer has made a strong showing that an employee has misappropriated confidential information and that such misconduct is likely to result in irreparable harm. This was the case in *Pharmerica, Inc. v. Arledge*, No. 08-CV-3939, 2007 BL 234119 (M.D. Fla. Mar. 21, 2007). There, the court ordered a former employee to turn over to the court all of the employee's computers, USB storage devices, hard drives, PDAs and other electronic devices. Significantly, the employer produced to the court evidence from a forensic analyst demonstrating that the employee had downloaded to a USB storage device, and then permanently deleted, hundreds of confidential documents in the weeks leading up to the employee's defection to a competitor.

  DLR ISSN 0418-2693

Conclusion

Employers can adopt several best practices to protect their most important customer, technical, and strategic information:

■ Insist that employees with access to confidential and proprietary information execute post-employment agreements that will protect that information from disclosure to competitors and other third parties.

■ Respond promptly to contain potential damages or losses that might be caused by departing employees, including notifying employees and their new employers of the employee's obligations under any post-employment agreements.

■ Where there is evidence that an employee has downloaded and/or obtained confidential/proprietary information, maintain a strict chain of custody for the employee's devices and consider promptly retaining a reputable and experienced forensic analyst to document and assess the extent of the employee's unauthorized access.

■ Should judicial intervention become necessary, demonstrate the specific harm that the company will suffer absent the requested relief by highlighting the scope of the employee's unauthorized access and any peculiar circumstances surrounding the employee's departure (e.g. downloading confidential documents immediately prior to joining a competitor).

Employee turnover is a fact of life for all companies. But, as discussed above, employers can take a number of measures to minimize the risk that confidential and proprietary information will ''leave the building'' with a departing employee and to put the employer in the best position possible to take action when an employee's misconduct threatens the employer's competitive advantage.