Bloomberg Law

Professional Perspective

Best Practices for Employers in Trade Secret Litigations

John P. Barry, Daryl G. Leon, and Meika N. Freeman, Proskauer Rose LLP

Best Practices for Employers in Trade Secret Litigations

Contributed by John P. Barry, Daryl G. Leon, and Meika N. Freeman, Proskauer Rose LLP

Trade secret litigations are not like all other litigations. In these cases, at least one party, if not both, need to advance their claims while carefully protecting the underlying information about which they are litigating—the trade secret itself. This heightened degree of protection necessitates particularized skill and care throughout all phases of the litigation to ensure that the trade secret is protected while the case goes forward.

A trade secret is generally defined as a combination of characteristics and components, each of which, by itself, may be in the public domain, but the unified process, design, and operation of which, in unique combination, affords a competitive advantage and is a protectable secret.

This article identifies best practices at a high level to help guide employers through the lifecycle of a trade secret litigation—from an employee's hiring through the completion of litigation. Although each topic discussed below could be the subject of its own article, this article seeks to familiarize employers to some key considerations for trade secret litigations before a fatal mistake, such as loss of trade secret protection, is made. The article is divided into two sections—company internal activities, such as hiring, internal procedures, investigations, etc., and external steps to protect trade secrets, such as cease and desist letters and court or arbitration litigation.

Company Internal Activities to Protect Trade Secrets

Employment: Confidentiality and Non-Competition Agreements

Employees can interact with a company's trade secrets on a number of different levels. On one end of the spectrum, employees may simply use the company's trade secrets so that they can perform their job duties. On the other end of the spectrum employees may be directly involved in developing, improving, or modifying the company's trade secrets.

In either case, employers best position themselves to protect their trade secrets when they can clearly and definitively point to an employee's understanding of and obligation to protect trade secrets. Most often this comes in the form of confidentiality provisions in an employment agreement, standalone restrictive covenant agreements, stock option awards that include confidentiality restrictions, and annual reaffirmations of an employee's obligations.

While a non-competition agreement is certainly one way to help protect trade secrets and confidential information, such agreements may not be appropriate, or even enforceable, for all employees and a non-competition agreement standing alone may not fully protect trade secrets. Indeed, in many states, using an overbroad non-competition obligation in place of a confidentiality obligation can lead to serious problems for employers. Further, a non-compete is not perfect for protecting trade secrets as non-competes have end dates but the value of the trade secret typically has no end date. Thus, a non-compete is not a substitute for a comprehensive confidentiality agreement.

Checks and Protocols

A notice of departure from an employee who has access to, or works with, company trade secrets should trigger certain checks and protocols. Depending on the nature of the employee's work, their exposure to trade secrets, and the timing of the employee's departure or employer's need for continued services, departing employees who work with trade secrets should ideally have their access limited and monitoring should be put in place for suspicious activities.

For example, to the extent it was permitted before they gave notice, a departing employee's ability to use thumb drives, digital upload services, such as Dropbox or Google Drive, and external email should be cut off. For high level, or high-trade secret access employees, the notice of departure may also trigger a hold on, or monitoring of, their email account and computer hard drive, so that the employer can check whether the employee accessed, sent, copied, or printed anything they should not have.

Just as during employment, a departing employee should be reminded of their obligations to protect the company's trade secrets. This may involve a discussion with the departing employee during an exit interview, sending them a written reminder, and communications with the departing employee's next employer to inform it of the departing employee's ongoing obligations.

Investigations

When an employer suspects that a departing or former employee has misappropriated its trade secrets, or as part of the off boarding process for certain sensitive employees, the first step is to conduct an investigation into the individual's activity while employed. This may involve examination of the employee's hard drive and email accounts, in addition to any other electronic devices the employer may possess, such as a cell phone or tablet, by the company's IT or HR department, or an outside forensic investigator.

The goal of any investigation should be to determine whether the individual complied with their obligations, or, for example, if they copied company files to a thumb drive, sent them to a personal email address, or used software to scrub their activities. In conducting the forensic investigation, employers should take care to ensure that the process does not mistakenly destroy the chain of custody or create similar questions about who actually engaged in the bad behavior. In other words, the forensic process should be conducted so that it does not over-write or create questions about what behavior was attributable to the former employee verses the company in conducting the investigation.

Incredibly, it is not uncommon during this process to find a smoking gun, clear proof that an employee created a folder, or sent an email to their personal email account, that identifies materials as company trade secrets. However, the lack of such smoking gun evidence is not fatal to an employer's claims, and indeed many cases are proved through the evidence developed during a subsequent investigation, such as a forensic review of the employee's personal computer or devices, or discovery in litigation.

Company External Steps to Protect Trade Secrets

Letters sent to a former employee or their new employer, and arbitration and court filings may become public. Thus, it is critical that from this step forward, the employer maintain the integrity and proprietary of their trade secrets—it should not be spelled out in any letters or filings, such as "we believe you stole our trade secret algorithm: X+Y-Z=Profit", at least until there is a comprehensive confidently order in place.

Cease and Desist Letters

Regardless of whether the employer located a smoking gun, the next step in trade secret litigation is often to send the former employee a formal cease and desist letter. The cease and desist letter serves multiple purposes, including to:

- Remind the former employee of their confidentiality and non-disclosure obligations and, in doing so, cite to any applicable agreements or company policies.
- Put the former employee on notice of the employer's allegations. For example, the cease and desist letter should identify the misappropriated trade secrets in a general matter and may reference findings from the employer's investigation, such as "you emailed these files to email address 'name@email.com' on your last day of work."
- State the employer's demands. The letter may demand the former employee return all company materials in their possession, turn over their personal devices or accounts for a forensic review, or identify all persons and entities with whom they have communicated about, or shared, the employer's trade secrets.
- Serve as a preservation notice. In doing so, the letter should demand that the former employee take immediate steps to preserve relevant information and documents.
- Cite to the applicable local, state, or federal laws that the employer believes the former employee may have violated.

The employer should also consider whether it is appropriate to send a cease and desist letter to the former employee's new employer. Such a letter may be appropriate if, for example, the employer believes that the former employee may be using its trade secrets at their new job. Sending a preservation notice to the new employer should also help future efforts to discover evidence that the former employee has introduced trade secrets into the new employer's computer systems.

Preliminary Injunction or Temporary Restraining Order

An employer may consider seeking a preliminary injunction or temporary restraining order against the former employee and/or their new employer. The likelihood of a court granting a preliminary injunction or temporary restraining order to

prevent the use or further dissemination of a company's trade secrets is substantially increased if the employer has uncovered forensic evidence that the former employee has misappropriated its trade secrets. However, as many cases require the development of evidence that would objectively demonstrate the unlawful behavior of the former employee and their new employer during discovery, an injunction may not be practical or feasible under the circumstances.

Court or Arbitration

Once the employer has determined to litigate its claims, it must consider where to do so. In many ways private arbitration provides greater protections for an accused former employee and employer, both of whom may not want their dispute litigated publicly. However, the parties may not have an arbitration agreement, or other considerations may render a court litigation more desirable.

Complaint

In drafting the complaint, the employer needs to include enough information to sufficiently identify the trade secret for the defendant and sufficient allegations to withstand or survive a motion to dismiss, without publicly disclosing the trade secret.

Confidentiality or Protective Orders

Regardless of the chosen forum, an employer should advocate early on for a strong confidentiality or protective order to ensure absolute protection of trade secret materials during and after litigation.

Although many courts and jurisdictions provide their own model protective orders, many of which offer strong protections, when litigating a trade secret case it is critical to understand the nuances of these litigations and anticipate circumstances that could jeopardize trade secret protections because a party cannot unring the bell if its trade secrets become public. The District Court for the Northern District of California, which has jurisdiction over Silicon Valley and sees a large number of significant trade secret cases, drafted a model protective order that is among the gold-standards for trade secret litigation.

Critically, any confidentiality agreement should provide for at least two levels of confidentiality –"Confidential" and "Highly Confidential–Attorneys' Eyes Only." The "Highly Confidential –Attorneys' Eyes Only" designation only permits designated counsel or select others to view extremely sensitive confidential information. This designation is particularly helpful to prevent the alleged misappropriator from being re-educated as to the employer's trade secrets during the litigation, or from exposing actual or potential competitors to the trade secret information.

Depositions and Experts

- Attendance at a deposition should be limited to individuals who are obligated to protect the trade secret information that they may learn.
- In line with the terms of the parties' confidentiality agreement, deposition attendees, including the witness and court reporter or videographer, may need to affirm their agreement to maintain confidently.
- Deposition transcripts should be appropriately marked for their confidentiality status.
- Selection of expert witnesses will need to strike a balance between exposing a new unrelated individual to a party's trade secrets and using the best qualified individuals to serve as experts. Depending on the circumstances, the parties should consider limits on an expert's subsequent use, reliance, and disclosure of the trade secrets, a preclusion on the retention of experts who actively participate in the employer's industry, or a prohibition of some kind on an expert's ability to work in the industry or sector.

Conclusion

Maintaining the confidentiality and propriety of trade secrets is an added burden on the parties to a trade secret action, but one which is essential. It requires careful thought and planning to anticipate the ways that litigation, if allowed to follow the regular course, may publicly expose a party's trade secrets, and planning to ensure that does not happen. For an employer that has spent time and resources developing and protecting trade secrets, the litigation concerning those trade secrets should be no less thoughtful or secure.