McKOOL SMITH
TRIAL LAWYERS

Client Alert

Legal Distancing: Reducing your odds of catching/spreading Trade-Secret litigation in the these tumultuous times

May 2020

Contact:

Robert Manley
Principal
McKool Smith
(214) 978.4226
rmanley@mckoolsmith.com

I. Introduction

These tumultuous times are an ideal breeding-ground for future trade-secret disputes. This paper offers best-practices to reduce your chances of becoming a part of one of those disputes, hopefully making the future easier for all parties. Understanding how busy things are, this paper is in a concise outline-form. If you would like more information, please contact us.

We believe that trade-secret litigation is likely to substantially spread with this crisis for several reasons. First, in the wake of 2008, there was around a 20% spike in civil litigation. Second, federal trade-secret filings were already increasing before the crisis: up 50% in the last 5 years. Third, the two main causes of trade-secret litigation are, regrettably, skyrocketing each week:

1. **New and former employees**: when a business's relationship with an employee begins or ends; and

2. **Business breakups:** when a business's current or prospective relationship with another business ends.[i]

Finally, these problems are compounded by both the increasing portability of information and the current shelter-in-place work environment. Even before SARS-CoV-2 ("COVID-19") moved workers home, more than 50 percent of employees saved work to external devices on a weekly basis.[ii] That number has no-doubt skyrocketed in recent weeks as workers setup home offices. In short, trade secrets are being spread outside of organizations at the very time companies are parting ways with employees.

Luckily, much like social distancing can stem the tide of COVID-19, there are hygienic practices that can reduce the chances of "catching" trade-secret litigation from either of the common causes (new and former employees or business breakups).

These recommended preventative legal-distancing practices are explained below following an overview of common problems in trade-secret litigation (to know what to avoid) and examples of common scenarios that lead to trade-secret litigation (to aid in recognizing a potential future dispute).

II. Common Problems in Trade-Secret Litigation

Before discussing specific best-practices, it is important to understand the common problems that arise in trade-secret litigation that we are trying to avoid:

1. **Whether a bad act was committed can be unclear.** Generally, a trade-secret claim involves a taking of protected information that is valuable because it is not otherwise readily known or easily ascertainable. Sometimes the taking is obviously deliberate (e.g., the crown-jewels are copied to a flash drive and a jet to a foreign country awaits). Other times, after the dust settles, it appears it may have been a misunderstanding (e.g., information was taken but it was not secret or was not valuable).

2. **There will probably be a fight to define what was taken.** Surprisingly, the most-common fight in trade-secret cases is over what the claimed trade secret is. In other words, what is it that the plaintiff contends was taken?

3. **Is it really a contract case?** Breach-of-contract claims are asserted in around 80% of trade-secret cases. And the parties' contract from their prior relationship often has a clause regarding the protection of confidential information. This can create sub-disputes over whether the trade-secret claim is freestanding or whether it is just a part of the contract claim.

4. **It will likely require technical expertise.** Trade-secret litigation can involve broad fights over the technology of an entire industry and are often as technical as a patent case (if not more so). This adds a challenge to communicating the issues to lay decision makers, including the court and jury.

5. **The defendant may never know what it is accused of.** In some cases, the claimed list of misappropriated secrets is itself classified as an "attorney's eyes only" secret document. This can mean that no one on the defendant's side, except outside counsel, can even see what the defendant is accused of taking. This can create substantial difficulties in discovery (e.g., how does counsel ask for the client's help if the claims are secret) and acrimony in the litigation (e.g., how can we know if it is a legitimate claim if they won't let us see it).

6. **Tensions will be high.** Trade-secret litigation claims a bad act that, in other circumstances, might be prosecuted as a crime. Press coverage may make the parties determined to vindicate their positions. And, if the defendant believes it took something substantial, it may be concerned that the evidence will implicate it in a crime.

III. Best Practices for Avoiding Common Trade-Secret Cases

Now that we know the common problems, we will discuss strategies for lowering the odds we encounter them. The strategies are grouped based on the two most common scenarios for trade-secret litigation: (A) the "Business Breakup," and (B) the "New and Former Employee."[iii]

A. The "Business Breakup"

1. Recognizing a potential "business breakup" case

The business-breakup case has two common forms: (1) a breakup after a long-term business relationship and (2) a failure to launch, where the proposed business venture never gets off the ground. The central problem is the same in each case—companies voluntarily exchange information without taking the time to clearly delineate what is a secret and what is not. After the relationship sours, the uncertainty over whether particular information was a secret becomes fertile ground for litigation claims.

Here are some detailed examples of business-breakup facts to aid you in recognizing a potential-problem scenario:

1. **The long-term breakup:** Business X and Business Y have been in a multi-year relationship. Y provides a service that is used at the competitive core of X's business, and the companies communicate closely. Y refines and improves its service (benefitting X's business) by seeing X's needs and listening to X's suggestions. Things are great, but then either Business X or Y brings another company into the picture.

    a. Business X is concerned by both the cost of Business Y's services and the risk of relying on Y. After all, the more X relies on Y the stronger Y's position in the relationship becomes and the more money Y can demand. Business X starts working with (or acquires) Business Z to reduce its exposure. Y learns it is being replaced, knows it has shared its secrets with X, and sues.

    b. Business Y improved components of its services (and developed new offerings) through its work with Business X. Liking money, Business Y provides these services to other companies, including competitors of X. Business X learns of Business Y's actions, remembers that the XY contract gives X ownership over their joint work, and sues.

2. **The failure to launch (e.g., M&A):** Business A says it is interested in buying Business B, so B provides information about itself to A. Hopes run very high (and a bright future is imagined by all), but the deal falls through, and B soon learns that A has developed something suspiciously similar, either after acquiring B's competitor or from rapid development in-house. Business B knows it shared secrets, has reason to believe this trust was violated, feels betrayed, and sues.

2. Legal-distancing strategies for the "business breakup"

Luckily, there are preventative measures that can reduce the likelihood of ending up in trade-secret litigation. For business-breakup scenarios, these measures revolve around the parties committing, via contract, to both reduce the ambiguity over whether exchanged information is secret and to be specific in any future dispute claiming misappropriated secrets. This approach may require a little bit more work in advance by the parties, but it is a case where an ounce of prevention is worth a litigation of cure.

i) For the "business breakup"

- **Agree to clearly designate confidential material.** Before any material is shared, the companies should agree to clearly designate every document they consider confidential with an agreed mark (e.g., similar to a protective order). The companies should agree that any document without such a mark is not confidential, though they may agree to allow after-the-fact designation (e.g., within 7 days). This will help reduce future disputes over whether a specific document was confidential.

- **Agree, if there is a future dispute, to mediation prior to suit, including a detailed identification of misappropriated secrets prior to the mediation.** The identification should include, if possible, a list of specific documents that are claimed as misappropriated secrets as well as a reasoned identification of the valuable secret portions of those documents. This transparency can facilitate a business-resolution to a case, including settlement.

- **Agree, if there is a future dispute, to allow the other side's in-house counsel to see the list of claimed secrets.** This will allow increased transparency in litigation and can facilitate a business-resolution, including settlement. Otherwise, the defendant company may not be able to know what it is accused of. For peace of mind, conditions can be placed on the in-house attorney's scope of responsibility (e.g., the attorney is not involved in patent prosecution).

ii) For the failure to launch

- **Use a clean room.** Make the use of a restricted-access "clean room" a mandatory part of the process. As part of the disclosure agreement, the offering company (Company B above) should require that confidential information will only be disclosed in a defined clean room. The potential acquiring company (Company A above) must agree that only specifically-named individuals can access this clean room and that they will not share confidential information with any other individuals.

- **Agree to the provisions for a future disputes described above.**

- **Agree to destroy all provided material.** The companies should agree to destroy all copies of information received after a set period of time (e.g., 90 days), unless there is a future agreement. This condition encourages companies to keep material organized, since they know everything must be destroyed. It also promotes peace of mind for both sides.

- **Avoid broad NDAs; try to enter agreements for specific information.** Many trade-secret cases germinate from short NDAs (e.g., 1-2 pages) that make *all* information exchanged between the parties confidential forever (or close enough). These agreements allow a party to later claim that any piece of information exchanged was a secret. If possible, only enter into narrow NDAs for specific documents (e.g., a yearly spreadsheet, a technical specification) for limited terms (e.g., 1-2 years).

- **The acquiring company should clearly document its own internal technology.** Before accessing the offering company's secrets, the acquiring company should clearly document its own internal progress in any related technological area. This documentation should be preserved in a secure way.

B. The "New and Former Employee"

1. Recognizing a "new and former employee" case

The new and former employee scenarios embody the truism that "trade secrets spread through people." The central problem in employee cases is that individuals leaving businesses often take information with them. While it is relatively easy for the business to know that information was taken, it can be a complex challenge to determine whether the information taken was valuable.

Here are some detailed examples of new-and-former employee facts to aid you in recognizing a potential-problem scenario:

1. **Employee leaves to a competitor:** Employee E works at Company C for a number of years and heads one if its technical departments. As part of joining the C, the employee agreed to a confidentiality agreement. One day, E tenders two-week's notice to C. After E leaves the company another employee notices that E now works for C's biggest competitor. News of this gets around the company and an employee reports to the general counsel that they saw Employee E copying file after file onto a flash drive the day she left. Company C believes its secrets were misappropriated and sues.

2. **Employee starts a competitor:** Employee E works at Company C for a number of years and heads its sales department. As part of joining the C, the employee agreed to a confidentiality agreement. One day, E tenders two-week's notice to C. Company C soon learns from a supplier that E has set up a competing business, is using the same suppliers as C, and is targeting C's customers. News of this gets around the company, and an employee reports to the general counsel that they saw Employee E copying file after file onto a flash drive the day she left. Company C believes its secrets were misappropriated and sues.

3. **Employee starts at your company:** Employee E is a former employee of Company C (and others). Employee E was hired by your company for her technical skills. Unbeknownst to your company, before leaving Company C, Employee E copied several files onto a flash drive. These files were mostly personal photos, but, in the background of holiday photos at Company C's offices, there are whiteboards full of technical information and even product prototypes. Company C learns Employee E copied files, examines its software records of what was copied, identifies the photos, and sues to recover its information.

2. Legal-distancing strategies for former employees

The preventative measures for employee scenarios revolve around reducing the likelihood that employees depart with confidential information and providing agreed upon mechanisms for giving the business peace of mind that nothing valuable was taken while attempting to maintain the privacy of the now former employee.

- **Perform exit interviews with departing employees.** Personnel should prepare for the interview by considering what information the employee had access to, the company's agreements with the employee, and any knowledge of the employee's future plans. As part of the interview, the employee should be reminded of their ongoing obligations to protect the company's information and to not retain company confidential information (in any form). The employee may be asked if they disagree with any of the obligations, and to sign an acknowledgment of the interview and of the employee's continuing obligations.

- **Consider restricting the information an employee may leave with.** Depending on the type of business it may be reasonable that an employee should not leave the company with any information. Alternatively, the employee may submit specific materials to the company that are cleared for removal.

- **Consider an agreement for a third-party to search the employee's devices.** Depending on the scope of the employee's access to company secrets, it may be appropriate to enter into an agreement with the employee that provides for an accredited third-party to forensically examine the employee's devices to ensure that no company secrets have been retained.

3. Legal-distancing strategies for new employees

- **Perform an onboarding interview.** This interview provides an opportunity to ensure that the employee is not bringing material from a prior employer into the company. The employee may be asked to sign an acknowledgment of the interview and a confirmation that they are not bringing in any confidential information.

IV. Conclusion

Businesses are making rapid changes in order to survive the current economic environment. This has resulted in an increased rates of employee turnover and folding businesses that have, in turn, heightened the risk of losing control over trade secrets. But this uncertain time will not last forever, and companies will assert control over their secrets, likely using litigation. Our hope is that the preventative measures suggested above will help you to avoid become a part of one of those disputes. If you have any questions, please contact us.

Robert Manley
rmanley@mckoolsmith.com
214.978.4226

Rudy Fink
rfink@mckoolsmith.com
214.978.4213

Jonathan Powers
jpowers@mckoolsmith.com
214.978.4088

[i] Current and former employees are the groups most often sued for trade secret misappropriation. *See* David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. REV. 291, 302-04 (2010) (*Federal Study*); David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in State Courts*, 46 GONZ. L. REV. 57, 68-71 (2011) (*State Study*). The next most sued group is business partners. *Id.*

[ii] OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE (2011) at A-3.

[iii] These two scenarios account for more than 85 percent of all federal trade secret litigation, and more than 90 percent of all state court trade secret litigation. *See Federal Study* at 302-03; *State Study* at 69.