HACKING YOUR NONCOMPETE

MINIMIZING THE RISKS OF TRADE SECRET MISAPPROPRIATION AMONG MOBILE EMPLOYEES

Gregory M. Stone, Esq.
Whiteford, Taylor & Preston L.L.P.
Seven Saint Paul Street, Suite 1500
Baltimore, MD 21202
Phone: 410-659-6402
Email: gstone@wtplaw.com

Hacking the Noncompete – Minimizing the Risks of Trade Secret Misappropriation Among Mobile Employees

1. Introduction

We live in a world enabled by technology. Ours is an increasingly knowledge- and innovation-based economy driven by innovative companies and their employees. Just as the corporate innovators compete with one another to get their products and services in the marketplace, they compete for the talent that drives the innovation in the first place; the tech employees that come up with the latest code, gizmo, or other innovation that keeps them competitive. Of course, most of those tech employees know their talent and value, and managing the mobility of such talented tech employees creates challenges. For the employer, there is the ongoing need to ensure that the company's secret sauce does not escape the walls of the company and find its way to a competitor. For the employee, there is the ongoing need to make sure that they can continue their career growth, building on the prior experience they've gained, while making sure they don't inadvertently step into claims of misappropriation of their former employer's trade secrets. For the new employer, there is the ongoing need for talent, which must be balanced against the risk of getting sued by a former employer for inadvertently taking in their trade secrets.

This paper explores the issues faced by such former and future employers and their tech employees as those employees move in response to the continuing demand for tech talent.

2. Pitfalls Created by Tech Employee Mobility

Tech companies employ and seek tech talent. In the ultra-competitive technology marketplace, tech employees are a rich asset. Losing key tech talent to a competitor not only causes the former employer to lose that person's skills that would be applied to new product development, but risks that the employee's move will take secret technology to a competitor, causing loss of investment in that new technology and increased and possibly unfair competition. If the information was not properly protected before the employee's departure (such as through agreements with the employee setting out obligations to keep information confidential and protecting against copying of information), the employee may either intentionally or unintentionally disclose that information to their new employer, and ultimately destroy the trade secret nature of the information. The new, hiring employer may likewise buy themselves a trade secret misappropriation lawsuit or an injunction (and the related costly legal battle) against hiring the new tech employee if there is risk that they will bring trade secrets that might be inadvertently disclosed or used in their work. And of course, the employee themselves risk burning the relationship with their prior employer, only to find themselves unemployable by their intended new employer, or even worse, sued for damages by their former employer.

Of course, giving rise to all of the foregoing risks is the presumption that the former employer has confidential, proprietary, and possibly trade secret information to start with that the subject employee had access to during their former employment. A trade secret is a specific type of intellectual property that, while certainly protectable, must meet certain qualifications in order to maintain its status as a trade secret. Specifically, a trade secret comprises any information that

has independent economic value to a company, that is confidential, and that is the subject of reasonable measures by the owner of that information to maintain its secrecy. Failure to take reasonable measures to secure confidential information, such as by limiting physical and electronic access to information to only authorized persons that must access it through appropriate security measures (passwords, physical locks, etc.), having persons that obtain such access sign confidentiality agreements, prohibiting third party devices from being used to copy or store data, and the like can result in a loss of any trade secret interest in that information. In this case, if the information that the employee takes to their new employer does not qualify for trade secret protection, and if the employee is not otherwise bound by agreement to keep such information confidential, the prior employer will find themselves unable to restrict their former employee or new employer from using that information.

Employers who fail to take appropriate action to prevent disclosure of their confidential and proprietary information thus risk loss of proprietary protections for that information, and a former employee and their future employee are free to use such now publicly available information without infringement or misappropriation liability. Former employers have been bitten in this way by, for example, not having employees sign a covenant not to compete. Absent such a covenant not to compete, or an actual or threatened disclosure of the prior employer's trade secrets, an employee is certainly free to pursue their chosen field of endeavor, even in direct competition with the former employer. Likewise, the former employer providing information to customers without obtaining an agreement by the customer to keep such information confidential can be problematic. If confidential or trade secret information is freely given to a customer or other third party, the former employee and their new employer are similarly free to use such information. Further, if the information is readily ascertainable from observation or from sources other than the former employer or the mobile employee's information, it should not constitute a trade secret of the former employer.

A very common and easily avoided pitfall created by former employers is simply failing to confirm and remind departing employees of their obligations to keep the former employer's confidential information in confidence. Often times, simply having a detailed exit interview that confirms their obligations and that gets agreement on what properly constitutes the prior employer's confidential and/or trade secret information can avoid having the employee either inadvertently or intentionally disclose or use that information at their new position.

Moreover, trade secret information is different from the general knowledge that an employee develops over time. Where the competitive information that a former employee and their new employer is using is already of general knowledge, at least in the relevant industry of the competitors, it cannot constitute trade secret information, and the employee and new employer are free to use that information. Likewise, information that the employee brought with them to the prior employer does not automatically become the confidential information and property of that employer. Absent some written agreement between the employer and the employee, the employee's prior information remains their property, such that they can freely use that information in their new employment.

Likewise, for inventions that were developed by the employee before their departure, if the former employer does not have a written agreement governing ownership of such inventions,

the former employee may be well within their rights to continue to use and commercialize such inventions, and even share them with their new employer. A common misconception among employers is that under the "work for hire doctrine," everything that an employee comes up with while working for that employer should belong to the employer. Not so!!! Work for hire is a doctrine under copyright law that dictates that the copyrightable works of employees that are created within the scope of their employment are the property of the employer. However, this only relates to the copyright interest in such works, and that such works be created by an employee (and not a contractor, in which case the ownership transfers automatically to the employer only in certain limited circumstances). Copyrights protect literal expression that is "fixed in a tangible form" – thus, for any computer code written by an employee, white papers written by an employee, or anything else authored or created by an employee within the scope of their employment and that is subject to copyright protection, the resulting copyright interest is owned outright by the employer. Such copyright interest allows the owner (i.e., the employer) to prevent others from making substantially similar copies of the copyrighted work. Importantly, however, it does not protect the ideas embodied in such copyrighted work. Thus, and for example, if an employee develops a new, software-implemented invention, while the code itself may be copyrighted and owned by the employer, the functions that the software performs are not protected by copyright. If the innovation embodied in such software rises to the level of a patentable invention, the employee owns that invention absent either a written agreement that requires assignment of the employee's inventions to the employer, or other, narrowly tailored employment situations where the employee was clearly hired to invent the specific thing that is being patented. Thus, absent a clear definition of the employee's role as one to invent, and/or obtaining written agreements with employees covering ownership of such employee-developed intellectual property, departing employees and their future employer may be freely able to use such information and inventions without liability to the former employer.

Of course, the new employer also faces potential legal pitfalls in taking in a tech employee from a competitor. In the event that the new employee brings confidential and proprietary information of their former employer and uses or discloses that information (either intentionally or inadvertently), the new employer could face liability for unfair competition claims and even misappropriation of trade secrets from the former employer. For example, if the new employer is a direct competitor that places the employee in a comparable position to their former position without restrictions against using or disclosing their former employer's trade secrets (which obligations should be in writing), they may open themselves to a lawsuit for an injunction against use of such information, and possibly even against continuing to employ that employee (in addition to damages for misappropriation of the trade secret). Likewise, if there is a document trail showing that the new employer sought out the new employee particularly because of their wealth of confidential information of the former employer, as opposed to simply seeking someone with general knowledge and skills in the industry, the new employer further increases the likelihood of liability. Moreover, where the new employer suddenly and "coincidentally" jumps into a new and lucrative market that they had not previously serviced but just so happens to compete directly with their new employee's prior employer, risk of liability for the employer is further increased. Still further, when hiring a new employee from a close competitor, new employers can find themselves at increased liability for simply failing to investigate their new employee's nondisclosure obligations owed to their former employer. While the existence of such obligations does not necessarily preclude hiring that employee, they

could suggest that job duties be carved out that avoid overlap with those prior obligations for as long as they last under a noncompetition agreement with the former employer, and failure to do so can again increase risk of liability for the new employer.

And while all of the above address risks faced by the employers, the employee likewise faces risks in moving from one employer to the next. They obviously have a technical skillset that is in high demand. But if that skill set is valuable to one company, it's certainly valuable to their competitors. If, in the excitement of starting a new job, the mobile employee blindly signs a broad noncompetition or other agreement, they may tie themselves to unnecessarily binding limitations. Such agreements must be reasonable in their scope and duration, but that is for a court or jury to decide after costly and often protracted litigation (for which positive outcomes are never a guarantee). If the mobile employee does not document their pre-existing intellectual property, they could quite easily step into a fight over who owns it later. If the mobile employee doesn't document their independently developed intellectual property that was, for example, created while moonlighting on other projects outside of time at work, they could again easily get into a fight over who owns it later. If the mobile employee inadvertently incorporates their prior employer's intellectual property into their new employer's new products, they could certainly face legal liability. Often, such mobile employees find themselves in hot water when they failed to recognize what constitutes "confidential" or "trade secret" information of their prior employer which they must keep in confidence at their new position. While general information relevant to the employee's technical field, and that is known in the industry, cannot be confidential or trade secret information (and is thus free for the employee to use in their new employment or elsewhere), any information of their prior employer that was not generally known, that the prior employer took measures to protect, and that provides them some economic advantage risks liability for the employee if disclosed or used in their new position. Failure to specifically identify what the prior employer considers as their confidential and proprietary information and trade secrets before departing their employment leaves the question open, which can allow the employee to inadvertently disclose or use that information in their new position. Further, where such mobile employees are moving to a competitor of their prior employer, failure to consider the new job title and responsibilities can increase risk of liability. Crafting a job description that clearly sets out differences from the prior job can be quite helpful in reducing this risk. Moreover, where the mobile employee signed a noncompetition agreement with the former employer and is being paid (such as through a severance agreement) through the noncompete period, it is obviously risky to accept offers for new employment in a competitive position before the end of that noncompete period.

Of course, one of the biggest pitfalls created by the mobile employee that is heading to a competitor to their former employer is acting in ways that objectively raise a flag of concern of fraud, deception, or other misleading conduct. For example, it is never a good idea to harvest confidential or proprietary information from the former employer onto electronic devices (e.g., making digital copies of customer lists, vendor lists, suppliers, business plans, technical notes, etc.) before departing the former employer. Doing so almost always leaves a detectable trail and generally suggests an intent to misappropriate the former employer's confidential and / or trade secret information.

Clearly, there a numerous pitfalls that are created for all parties involved when a tech employee changes employment. Nonetheless, through careful advance planning, those pitfalls can be managed in a way that protects the interests of each of the former and new employers and the mobile employees themselves.

3. Tools to Safeguard Against Liability for the Disclosure and Use of a Former Employer's Confidential Information

The list of risks associated with tech employee mobility can seem daunting, but there are certainly measures each party can take to minimize the risk of liability when a tech employee moves among competing employers.

From the perspective of both the former and new employers, physical and electronic infrastructure should be engineered to minimize the risk of trade secret misappropriation, whether intentional or unintentional. For example, employers should have clear policies and electronic infrastructure that protect against making copies of sensitive documents and files.

From the former employer's perspective, it is wise to have an understanding with the mobile employee regarding the specific subject matter that falls within the scope of that former employer's confidential information and trade secrets. While the former employer might wish to use sweeping descriptions to minimize the risk of competition, doing so not only unfairly restricts the employee's ability to make a living, but also risks unenforceability by attempting to control use of non-confidential information. By having both the former employer and the departing employee agree on the specific subject matter that is off limits, misunderstandings can be avoided. Of course, clear noncompetition agreements that are clear and reasonable in scope and duration can go a long way in meeting that goal. Likewise, the former employer should ensure that information that it intends to hold as a trade secret is maintained in fact as a trade secret – i.e., such information (which has independent economic value to the employer) is protected through measures that restrict access, with its disclosure covered by appropriate confidentiality agreements. Technology tools and policies that an employer can use may include, for example, (i) computer safeguards (e.g., protecting computer systems with passwords that must be changed at regular intervals, firewalls, hard drive encryption, access logs and notifications, etc.); (ii) security measures for electronic technologies that employees might bring to the workplace (e.g., USB drives, flash memory cards, smartphones, access to social media sites, etc.); (iii) rules and restrictions governing access to and use of systems that hold confidential information; (iv) policies governing use of the employer's property (e.g., computer systems), generally; (v) policies for handling, labeling, and destroying physical documents; and (vi) policies for sharing information with third parties. Employers should also ensure that their workforce is educated to such policies (such as through meetings, employee handbooks, online mandatory training sessions, etc.), are subject to noncompetition agreements where appropriate, and go through a comprehensive exit interview before departing to ensure that each party is clear as to their respective rights and responsibilities. Likewise, records must be maintained that clearly set out such policies for securing that information, as the employer may be called on later to prove that they employed reasonable efforts to protect their information. To avoid questions of who developed such information and new technology, and when, where and how it was

developed, employers should document and maintain clear records of all significant developmental efforts.

From the new employer's perspective, it is wise to document (in an agreement with the new employee) restrictions against using or disclosing their former employer's trade secrets, which can help to establish that both the new employer and the mobile employee are acting in good faith to avoid any misappropriation. Likewise, it will be helpful for the new employer to understand and document the nature of the incoming employee's prior employment, and use that understanding to create a job description and duties that steer, as much as practicable, away from their prior responsibilities. Further, where the incoming mobile employee was not previously required to sign a noncompetition agreement, the new employer should not be bullied into not hiring the employee merely on assertions from the prior employer of some proprietary interest – rather, the specifics of any alleged confidential information must be evaluated to ensure that the new employee avoids situations that might inadvertently disclose or use such confidential information (e.g., by carving out job duties for the incoming mobile employee that are noncompetitive with their prior duties at their former employer).

Finally, from the mobile employee's perspective, while they obviously should be careful not to take copies of confidential information from their former employer or offer their new employer details of the inner workings of their competing prior employer, they likewise should not be bullied into over-restrictive provisions that would limit their ability to freely move to better career positions. For example, "general knowledge" cannot constitute a trade secret, as it is not secret information. It is thus helpful for such mobile employees to maintain logs of public information, resources, open source code, and the like that they use in their work so that they can readily establish the public nature of those materials. Likewise, for mobile employees that have developed their own intellectual property in a field related to their employment but outside of the scope of their employment, maintaining documentation showing the development process can help to establish that intellectual property as their own, and can help protect against an employer claiming it to be such employer's property. Moreover, the mobile employee cannot be prohibited from pursuing a livelihood in their chosen field altogether, and bully tactics by a former employer should be screened against a reasonableness filter (in both scope and time) before conceding to overreaching demands. As noted above, it is best to have a reasoned discussion with the former employer before departure that clarifies the former employer's understanding of what constitutes their competitive field and their confidential information, and hopefully have a written severance agreement confirming the same.

4. What to do When the Sharks Come Calling

Hopefully, by using the tools discussed above, both the mobile employee and the new employer can significantly reduce the risk that they will be faced with claims of misappropriation of trade secrets or the like. However, in the highly competitive space of cyber technologies, skilled employees are at a premium, which raises the risk that there might be a fight among close competitors over transitioning employees.

First, as noted above, the prerequisite to any claim of misappropriation of a trade secret is that the information actually be a trade secret. Thus, when faced with a claim of

misappropriation of such trade secrets or confidential information, it can be helpful to establish that the information is simply not confidential – i.e., that it comprises information that is already publicly known. Again, an employee's maintenance of records of third party resources used in the development process can help to establish the public nature of such information. Likewise, if the former employer failed to take reasonable measures to maintain the secrecy of such information, they may have no protectable interest to assert. Thus, a defendant faced with such claims may want to look to establish that the former employer has allowed third parties (e.g., customers, affiliated / partner companies, suppliers, etc.) to freely access that information without obligations of confidentiality, which would preclude its status as trade secret information. And where it appears that the former employer has sufficient grounds to support their claim to trade secrets, it may be advisable to seek to mitigate any damage by building an administrative wall around the new employee to ensure that ongoing duties are as separated as possible from the common, competitive area to which the trade secret relates.

Further, when faced with claims of breach of a noncompetition agreement, a review of the agreement itself is warranted to evaluate whether it is reasonable in scope and duration. It is not at all uncommon for courts to consider overreaching noncompetition agreements as unenforceable for being too restrictive against the employee's ability to pursue a livelihood. And still, even where the noncompetition agreement seems reasonable, former employers may simply wish to minimize competition and thus construe the provisions of such agreements as having a reach beyond what is spelled out in the agreement. In this case, it would be appropriate for the new employer and the employee to consider whether such claims by the former employer rise to the level of intentional interference with their contractual relations, and answer any overreaching threats of litigation for breach of the agreement with their own threats of a counterclaim seeking damages for that intentional interference.

More generally, in situations where a skilled tech employee subject to noncompetition provisions is moving to a competitor, both the employee and their new employer should start considering the implications of any restrictive covenants from the time the employee starts to consider leaving their current position. All actions from that point forward should be undertaken with the restrictive covenants in mind so as to minimize the risk of liability if the former employer takes action. Starting with the exit interview with the former employer, while it is best to be as candid as possible, it is critical for the mobile employee to carefully consider the questions presented and be cautious with their response. For example, while the mobile employee should expect that they will be required to acknowledge certain restrictive covenants, they should be careful not to simply accept legal or factual positions of the former employer without fully evaluating the potential consequences of agreeing to them. Likewise, for the new employer, they should obtain a clear understanding of the scope of the mobile employee's restrictive covenants and ensure that a job description and duties can be defined that avoid those restrictive covenants as much as possible. And if, despite their best efforts to avoid a conflict, the prior employer files suit, evaluate and assert all available defenses, which might include:

(i) The information that the former employer complains has been misappropriated is, in fact, not a trade secret or confidential information, but is rather general knowledge well known in the industry;

(ii) The employee's position changed over time with the former employer, such that the noncompetition agreement originally signed was no longer relevant to their duties at the time that they departed;

(iii) An agreement entered into as the employee is departing is not supported by separate compensation or other consideration;

(iv) There is no irreparable harm or injury that the former employer will incur as a result of the mobile employee moving to the competing new employer;

(v) The potential harm to the mobile employee created by the noncompetition provisions outweighs the potential harm to the former employer;

(vi) The new employer is not in fact a true competitor of the former employer;

(vii) The mobile employee's duties do not fall within the specific restrictive covenants set forth in their noncompetition agreement with the former employer;

(viii) The former employer simply waited too long to take action, giving the employee and their new employer the justified belief that it was safe to proceed with the new employment;

(ix) The former employer buried the restrictive covenants in another, otherwise unrelated agreement with the employee;

(x) The former employer has previously only selectively enforced identical noncompetition agreements;

(xi) The junior or low-compensation level of the employee makes a restrictive covenant unreasonable, even though it would be reasonable in the context of a higher level employee; and finally

(xii) That enforcement of the restrictive covenants against the mobile employee are simply unfair.

In any case, all parties are typically best served by avoiding costly litigation from the start, which hopefully can be accomplished by using the tools described above, which should help ensure that all parties have a common understanding as to the scope of each parties'

confidential information and their respective rights and responsibilities relating to that confidential information.