PUBLICATION

Trade Secret Protection Plans Provide Certainty to Employers

Authors: Hannah Elizabeth Jarrells, Edward D. Lanquist, Jr
May 22, 2024

Baker Donelson recently published an article called "The End of Non-Competition Agreements? Not so Fast!" The article summarizes the Federal Trade Commission's (FTC) final rule prohibiting most employers from binding the majority of American workers to post-employment non-competition agreements (Final Rule).

While the Final Rule's enforcement is expected to be delayed and will likely never take effect, the Final Rule itself is a good reminder that non-compete agreements in the employee-employer context are under more scrutiny than ever and in some states, like California, Minnesota, North Dakota, and Oklahoma, are already banned as a matter of law.

Other states, such as Colorado, Washington, Oregon, and Illinois, only allow employers to bind highly compensated employees to traditional non-competition agreements. Even in states that are considered to be employer-friendly in the context of non-competition agreements, judges are carefully reviewing non-competition agreements to ensure that they are reasonable in their duration, scope, and geography and are no broader than necessary to protect the employer's legitimate business interests.

The protection of trade secrets has long been understood to be a legitimate business interest, and, traditionally, companies have used non-competition clauses, along with other restrictive covenants, to protect their trade secrets. The rationale is that a non-competition agreement would prevent an employee with access to trade secrets from disclosing those trade secrets to a competitor or using those trade secrets to gain an unfair competitive advantage in the marketplace. Now, with non-competition agreements in doubt and facing greater scrutiny, companies will need to rely on other protection mechanisms.

However, the use of other traditional types of restrictive covenants, such as customer non-solicitation and non-disclosure agreements, may not be sufficient to provide the type of robust trade secret protection employers need. For example, the Final Rule states that if the enforcement of non-disclosure or non-solicitation provisions would substantially inhibit an employee's ability to work for a competitor, then such provisions are also void and unenforceable. Moreover, post-employment customer non-solicitation agreements are banned as a matter of law in California and some states, like Illinois, limit the types of employees who can be lawfully restrained by a post-employment customer non-solicitation agreement. In sum, restrictive covenants may fall short of providing the level of protection employers need. As a result, companies are more dependent than ever on trade secret laws to protect against misappropriation.

Specific statutory protection for trade secrets is found at the federal level with the Defend Trade Secrets Act (DTSA) and in most states with the Uniform Trade Secret Act (UTSA). To be a trade secret under either the DTSA or UTSA, the information must be of value to the company, derive value from the fact that it is secret from the company's competitors, and be subject to reasonable attempts by the company to keep it confidential. Additionally, the information cannot be commonly known or outdated.

Therefore, companies should implement a trade secret protection plan to ensure that their trade secrets are secure and that they can seek protection under the DTSA or UTSA if needed. The first step of any protection

plan is to determine what information constitutes a trade secret, where materials containing trade secrets are located, and who has access and needs access to the trade secrets.

Next, the plan should detail the exact steps a company will take to keep its trade secrets secure and confidential. An effective trade secret protection plan includes steps such as:

1. Having confidentiality and non-disclosure provisions in all employment contracts and requiring all employees to agree to the same as an express condition of employment;
2. Having confidentiality, non-disclosure, information security, and lawful electronic monitoring policies and protocols in employee handbooks and having employees acknowledge in writing that they have received, reviewed, and understand all such policies;
3. Providing training at the outset of employment and on an annual basis on: (i) the company's confidentiality, non-disclosure, and information security policies and protocols, and (ii) the importance of protecting trade secrets to maintain the company's ability to compete in the marketplace and allow the company to honor its obligations to keep customer and other third-party information confidential;
4. Having reporting and investigative policies and protocols in place to quickly and thoroughly investigate allegations of misappropriation;
5. Disciplining employees, including up to termination, for violations of non-disclosure, confidentiality, and information security policies and protocols;
6. Adding password protection to all company-owned devices and systems containing trade secrets;
7. Requiring that passwords meet length and complexity requirements and are changed on a regular basis;
8. Limiting access to files containing trade secrets to only employees who actually need such access to perform the duties and responsibilities of their jobs;
9. Ensuring that the company has the necessary policies and technology to lawfully record: (i) the identity of each employee who electronically accesses files containing trade secrets; (ii) the date and time of the access; and (iii) the employee's subsequent use of the trade secrets such as downloading, uploading, emailing, printing, modifying, etc.;
10. Ensuring that the company has the necessary policies and technology to lawfully monitor employees' electronic activity including the use of email and file transfer systems;
11. Using two-factor authentication or other enhanced security measures to protect files containing trade secrets;
12. Making certain that physical areas of the company where files or documents containing trade secrets are stored are equipped with adequate physical security measures such as locks and limiting access to those areas;
13. Clearly marking documents and files as confidential; and
14. Promptly disabling a departing employee's ability to access files containing trade secrets.

Protection plans do not need to be complicated to be effective. Indeed, it is much better to have a functional and easy-to-implement protection plan than a complex plan that is never fully operational. Further, a protection plan is essential in trade secret misappropriation litigation where employers are required to demonstrate under the DTSA and UTSA all of the steps the company took prior to the alleged misappropriation to protect its trade secrets. If a company cannot meet this burden of proof, then it cannot use the DTSA or UTSA to protect itself from misappropriation.

Companies need to begin the process of reviewing and revising their current trade secret protection plans now. If you would like to learn more about a trade secret protection plan, please contact Edward D. Lanquist, Hannah Elizabeth Jarrells, or your Baker Donelson counsel.