A World Without Noncompetes: Protecting Confidential Information and Trade Secrets

Employers should consider reassessing their protection efforts and focus to prevent unauthorized movement of information rather than the movement of employees who may have access to such information.

By Chris Larus, David Prange and Rajin Olson | February 22, 2023

A noncompete agreement is one of several tools that businesses may use to prevent the unauthorized dissemination of confidential and trade secret information to competitors. In recent months, however, the Federal Trade Commission has proposed a new rule to ban noncompetition clauses, reasoning that such limitations restrict worker freedoms and harm competition. Anticipating that this proposed rule will be put into effect, the change provides businesses a good opportunity to assess their protection strategies employed for company trade secret and confidential information.

The FTC's comments regarding its proposed new rule acknowledge concerns that the elimination of noncompete agreements could impact the protection of confidential information. In some (but not all) states, a business could rely on a noncompete agreement with an employee to act as a blanket protection from the unauthorized use of trade secret or confidential information if the employee would leave the company. The reasoning is that such information is effectively protected because the employee cannot move to other employment in which the information may be used to the detriment of the past employer.

The concern presumably underlying the FTC's proposed rule is that the noncompetition agreement unnecessarily restricts more activity than necessary to achieve the protection of confidential or trade secret information. In justifying the proposed rule, the FTC has asserted that employers have alternative strategies to protect confidential or trade secret information, namely trade secret and contract law involving non-disclosure agreements. In view of this expectation underpinning the FTC rule introduction, employers should consider reassessing their protection efforts and focus to prevent unauthorized movement of information rather than the movement of employees who may have access to such information.

Alternative Strategies to Protect Confidential Information: Trade Secret Protection Assessment and Planning

Legal strategies employing trade secret law (via the federal Defend Trade Secrets Act or state implementations of the Uniform Trade Secrets Act) to protect proprietary information are presumably unaffected by present FTC rule-making. In view of noncompete options potentially being eliminated, companies may consider assessing whether their remaining efforts to protect information are sufficient to meet or exceed the "reasonable measures under the circumstances" that those statutes require. To the extent a company's assessment of its steps to protect trade secret information is found lacking, the company might consider implementing additional protection measures. Failing to do so could result in a finding, when asserting the alleged trade secrets, that the unimplemented measures demonstrate the company did not take "reasonable measures" to protect its trade secrets. Such a finding could result in a misappropriating employee—and their new employer—escaping with no liability at all.

Successfully assessing and systematizing trade secret protection is more easily achievable with a plan.

While not required as part of reasonable measures to protect a trade secret, planning may be useful to inform present employees of the protected confidential information and steps taken to protect that information, as well as to provide future employees historical context of the information's protection. Additional steps for protecting confidential information may be tailored to the specific nature of a company's trade secrets and to the geographic areas in which the company does business. Planning could address information categorically or with greater specificity. The measures to be taken may address the industry and business risks specific to the business, while avoiding implementation based on overly-generalized assumptions of business risk.

For many businesses, a protection plan may consider (1) restricting access of sensitive information to only those with a need relating to their employment roles; (2) employing physical, digital, and geographic limitations on access; (3) complementing physical protections with contractual limitations on information use; and (4) implementing an employee education cycle from hiring to termination that reinforces the value and company protection of trade secret and confidential information. Generally, action is better than no action, particularly if after assessment a company determines that additional protective measures should be implemented, and a lack of action or planning may be used by an employee as an indication that information used during work is not company confidential or trade secret information. Small steps taken now may translate to potentially eliminating a larger loss later, when loss recovery is much more costly and less certain.

Alternative Strategies to Protect Confidential Information: Non-Disclosure Agreements

FTC rule-making also, presumably, will not reach regulation of non-disclosure agreements (NDAs) per se. In general, an NDA creates an enforceable contractual obligation on the part of an employee to protect and prevent the disclosure or misuse of company confidential information inconsistent with the employee's role. Companies should beware, however, that certain NDA provisions may be found unenforceable under the FTC's proposed rule.

First, an agreement may bundle several rights and obligations together, such as a non-disclosure provision, a nonsolicitation provision, and a noncompete provision. Absent a severability clause in the agreement, a bundled agreement may be found wholly unenforceable if the noncompete provision is eliminated. Second, the FTC has commented that "NDAs that are unusually broad in scope may function as de facto noncompete clauses, hence falling within the scope of the proposed rule." The FTC has compared such NDAs to more favorable NDAs that "may prevent workers from disclosing or using certain information, but they generally do not prevent workers from working for a competitor or starting their own business altogether." Thus, an NDA's overly broad protectionary language may result in a finding that the non-disclosure provision really falls into the noncompete category, making it unenforceable.

In view of the FTC's potential rule implementation, companies should consider a review of existing agreements to eliminate potentially unenforceable provisions. Problematic existing contractual provisions may be mitigated by entering into new agreements with key company employees.

Conclusion

The FTC's ban on noncompete agreements may affect some companies' efforts to protect confidential or trade secret information. Anticipating implementation of the FTC's proposed rule, companies may consider focusing on trade secret and confidential information protection efforts directed to the information itself and not on the individuals that use the information. Such an approach may mitigate future risk if existing information protection measures focused on the restriction of employee movement are found to be unenforceable.

Chris Larus *is a partner in the Minneapolis office of Robins Kaplan and the chair of the firm's national intellectual property and technology litigation practice.*

David Prange *is a partner in the firm's Minneapolis office and leader of the trade secret litigation practice.*

Rajin Olson *is an associate in the firm's Minneapolis office.*
