A World Without Non-Competes: Protecting Confidential Information and Trade Secrets Following the FTC's Ban

As a result of the FTC's ban of non-compete agreements, businesses should assess alternative ways to protect their confidential information, and may consider the use of trade secret and confidential information protection efforts directed to the information itself, and not the individuals that use the information.

By Chris Larus, David Prange and Rajin Olson | April 30, 2024

(This article is an update from its original version, published February 22, 2023 in The National Law Journal© 202X ALM Global Properties, LLC.)

Non-compete agreements have been among the tools businesses often rely upon to prevent the unauthorized dissemination of confidential and trade secret information to competitors. On Tuesday, April 23, 2024, however, the Federal Trade Commission publicly announced a long-anticipated rule banning non-compete agreements, claiming that such agreements restrict worker freedoms, suppress worker wages, and harm competition. The rule will ban all future non-compete agreements as an unfair method of competition. Existing non-competes would be deemed not enforceable, except for those impacting "senior executives," defined as workers earning more than $151,164 who are in a "policy-making position."

The rule is scheduled to take effect as early as late August. Extensive litigation is expected around this rule, and at least one challenge was filed in federal court the same day that the rule was announced. Although it is possible the FTC's rule will be struck down someday, businesses currently relying on non-compete agreements to protect their trade secret and confidential information face the risk that this rule will take effect. Barring court action striking down the rule, the FTC's recent action will require many businesses to reassess their protection strategies for company trade secret and confidential information.

The FTC's comments regarding its new rule acknowledge concerns that the elimination of non-compete agreements could impact the protection of confidential information. In some (but not all) states, a business could rely on a non-compete 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 articulated concern underlying the FTC's rule is that non-competition agreements unnecessarily restrict more activity than necessary to achieve the protection of confidential or trade secret information. The FTC has also estimated that banning non-competes will have substantial positive effects for "workers, businesses, and the economy," including an estimated 17,000-29,000 more patents each year, increased start-ups, reduced healthcare costs, and higher wages for certain employees. 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, 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 largely unaffected by the FTC rule. In view of the FTC's attempt to ban non-compete agreements, companies should assess whether their remaining efforts to protect information are sufficient to meet or exceed the "reasonable measures under the circumstances" that those statutes require. 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

The FTC rule 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 non-solicitation provision, and a non-compete provision. Absent a severability clause in the agreement, a bundled agreement may be found wholly unenforceable if the non-compete provision is eliminated. Second, the FTC has commented that "NDAs that are unusually broad in scope may function as de facto non-compete 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 non-compete category, making it unenforceable.

In view of the FTC's recently issued rule, 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 non-compete agreements may affect some companies' efforts to protect confidential or trade secret information. Anticipating implementation of the FTC's announced 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.*

This article updates an article originally published in the February 22, 2023 edition of The National Law Journal