PUBLICATION

Guardians of the Goldmine: Building an Effective Confidentiality Program

Authors: Theresa M. Sprain, Edward D. Lanquist, Jr
August 15, 2024

On August 14, Judge Corrigan for the Middle District of Florida, in *Properties of the Villages vs. FTC,* found that the FTC did not have the authority to enter its planned Noncompete Rule, and entered an order granting an injunction as to the plaintiff only. Like the Texas federal court in *Ryan*, the court declined to grant a nationwide injunction. With yesterday's decision and the recent decision in *ATS Tree Services* denying the plaintiff's motion for preliminary injunction in part due to the FTC's likelihood of success on the merits, the only remaining legal obstacle to the implementation of the FTC Noncompete Rule is the *Ryan* court's merits decision on the Rule, expected no later than August 30, 2024. These developments make it imperative that businesses across industry sectors including, energy, financial services, health care, manufacturing, technology, telecommunications, retail, and hospitality, to evaluate improvements to existing plans to protect competitive and confidential information.

In our last alert, we focused on the value of audits as a core action in any robust protection plan to ensure maximum security and protection of your trade secrets and confidential information. Once that key information is gathered, every company needs to ask itself: if the FTC's non-compete ban ultimately takes effect, is my business as protected as it can be from unauthorized access, misappropriation, and misuse of my valuable confidential information?

If the answer is anything other than an unqualified "yes," the next step should be determining how you can improve the protections available to the company. Successful companies will employ a multidisciplinary approach to legally protecting confidential information that involves a combination of business initiatives. This is a topic we will explore in more detail during a webinar we are hosting on August 27, titled, "Preparing for September 4: Protecting Your Company's Trade Secrets, Competitive Edge, and Goodwill Amid the FTC's Ban on Non-Competition Agreements." Click here to register for that program.

While any combination of policies, training, physical and electronic security controls, and agreements can be effective, the most successful approach will be one that looks at these various tools as part of an overall program designed to create a culture of confidentiality, security, and compliance.

Through the issuance of its Noncompete Rule, the FTC has sought to eliminate the use non-competes. According to the FTC, overbroad non-solicitation clauses limiting an employee's post-employment rights to solicit other employees, vendors or customers, to the extent that they function as non-competes, will also expose employers for violating the new rule. The audit recommended in our last alert, therefore, will inform companies about the current status of their protections. The next step should be to ask whether and how those current protections can be reasonably expanded and improved.

A next-generation plan should include coordinated feedback from multiple organizational groups. The effort should involve legal counsel to ensure, to the extent available, that the deliberative process is protected by the attorney-client privilege. But any such effort should also include a combination of the following, depending on the company's individual business structure and need: business and finance personnel familiar with the competitive nature of business information and how it is treated in the industry; information technology and

security (IT & IS) to discuss the systems and processes that are already in place or which could be deployed; and human resources to cover any employee training, policies, or agreements in place or which could be revisited. Each perspective – legal, business, finance, security, and human resources – provides a critical lens through which these issues must be viewed.

After an audit, those constituencies should be brought together to address the foundational question: how do we design a legal and reasonable plan to protect our competitively sensitive confidential information? The topics to discuss will be heavily dependent on the company's nature, scope, and offerings, the particular business environment, industry norms, and available technology and resources. The constituencies should address:

- **Categories of Protectible Information**. What confidential information does our company own and, by ranking, what is the most important category that our business depends upon?

- **Operational and Human Resource Policies**. Do our company's current policies accurately address the operational and business needs of our business and sufficiently protect our varying categories of confidential information? This should include all applicable policies, including systems and property access, personal use of company systems and devices, use of personal devices, and social media policies. Are our policies in line with other applicable laws, such as the National Labor Relations Act requirements?

- **Cybersecurity Policies**. Do our company's physical and logical security protocols and processes address the varying categories of confidential information adequately, or is there room for improvement through the use of re-design or additional tools? Where are the most substantial threats of exfiltration for this information? Has the company reasonably limited access of competitively sensitive information to those employees who need it to perform their essential job functions?

- **Training Implementation and Execution**. Has our company sufficiently trained its employees around the value of confidential information, or does new and revised training need to be implemented? Does our training accurately and adequately express to employees (and, in particular, supervisors) why confidential information and trade secrets are critical to the company and the employees?

- **Nondisclosure Agreements**. Do the company's nondisclosure agreements comply with applicable law and do they sufficiently cover the competitively sensitive information adequately, both with employees and any other parties necessary to the business, such as vendors and customers? These agreements serve to reinforce and acknowledge the confidentiality and security policies of the employer but also create a legal framework to protect data and ideas from being shared or disclosed to third parties. As such, it is critical for companies to consult with counsel to ensure their agreements are enforceable under the state or states' law are most likely to be applied in the event of a dispute.

- **Non-solicitation Agreements**. Has the company created and enforced reasonable non-solicitation agreements that are compliant with applicable law, do not overly burden employee mobility, and protect relationships essential to the company's business? If you are not currently utilizing these types of agreements, now is the time to consult with counsel. If you already have such agreements in place, review them with your counsel to ensure they are enforceable, and like nondisclosure agreements, with applicable state law.

- **On-Boarding and Off-Boarding Protocols**. Does the company have a policy and protocol for incoming and exiting employees designed to protect confidential information? Discussion of these policies will likely bring to surface business operational issues, such as creating redundancies to ensure no customer, system, or project is solely addressed by one employee.

- **Antitrust Policies and Guidance**. Does the company need to update its antitrust compliance policies and program to ensure that the company's employees understand the requirements around antitrust and employees?

- **Interactions with Labor Competitors, Including Information Sharing and Benchmarking**. What interactions, either formal or informal, does the company have with competitors for labor? This could include information sharing or benchmarking, or contacts with competitors that could be interpreted as no poach agreements. The antitrust agencies and plaintiffs' antitrust bar have targeted industry information sharing arrangements and alleged “no poach” agreements. The antitrust agencies have recently revoked long standing antitrust guidance setting out “safe harbors” or “safety zones” for benchmarking.

- **Antitrust Policies, Training and Guidance**. Does the company need to be updating its antitrust compliance policies and training program to ensure that the company's employees understand the requirements around antitrust and employees? Should employees be getting mandatory regular training to emphasize the importance of antitrust compliance?

In the event that companies need to act to enforce their rights, contractual or otherwise, against an employee, competitor, or otherwise, advance efforts such as those outlined above in terms of creating a plan that designates, contains, and monitors confidential information and trade secrets will be critical evidence of their legal status and their value to the company.

In short, companies should reevaluate the entire program – both individually and the overall "fit" of the program – with the various constituencies to ensure that it works well overall. Advanced planning will help you see opportunities to improve your systems now and prevent you from discovering them in an emergency.

Baker Donelson will continue to monitor and update on developments associated with the Non-compete Rule, which remains set to take effect on September 4. If you have any questions, please contact the authors or a member of Baker Donelson's Intellectual Property or Labor & Employment teams.