PUBLICATION

Trust, but Verify: The Power of Audits to Protect Your Competitive Edge as Non-Compete Ban Looms

Authors: Jennifer L. Anderson, Adam Baldridge, Nicole Berkowitz Riccio
August 12, 2024

Corporate leaders concerned about protecting the recipe for their company's success have been following the fitful path of the FTC's rule banning non-competes. Lawsuits seeking to enjoin the rule were filed in multiple courts, but preliminary rulings conflict with the rule's legality and have offered no clarity about its ultimate fate. It remains set to take effect on September 4. Baker Donelson will be hosting a multi-disciplinary panel on August 27 to discuss the impact of the FTC's ban and its practical implications for companies determining how best to legally protect their confidential information and trade secrets.

Previously, Baker Donelson issued guidance about what businesses can do now to protect what matters most – regardless of the future of non-competes. Non-competes are not the only or even the most effective way to prevent losing customers and revenue. Companies across all industries, including energy, financial services, health care, manufacturing, technology, telecommunications, retail, and hospitality, must above all be proactive and programmatic in identifying and guarding the non-public ideas, strategies, plans, customer lists, documents, data, and other valuable information that uniquely makes them tick. This information may qualify for protection as a trade secret – a specific type of confidential information protected by federal and state trade secret laws – or may be protected under various types of contracts, such as confidentiality, non-disclosure, and employment agreements; corporate policies and employee handbooks; and other laws that create obligations arising from employment relationships. Regardless of the legal theory, the business must be able to prove that it took reasonable steps to keep its information confidential and reasonably and properly protected its trade secrets. Proving reasonable steps requires both a plan *and verification* that the plan is operating effectively.

The primary way to verify that a protection plan is working is by conducting routine audits, which also help create a culture of confidentiality, security, and compliance. Auditing should involve a group or team – avoid siloed employees who can act without checks or balances –responsible for reviewing that protocols have been implemented, are being followed, and are shored up against potential weaknesses and breaches. Companies should create an audit checklist identifying the auditors, items reviewed, and actions taken, as well as the dates and other details for each audit conducted, which for all items should occur at least annually. Consider including the activities below in your checklist, which can be used along with the list of plan-creation steps we suggested in our prior guidance.

1. Review personnel files to verify they contain current and executed policy acknowledgments, training certificates or confirmations, employment contracts, confidentiality and non-disclosure agreements;

2. Review contractor and vendor files or records to verify they contain current and executed confidentiality and non-disclosure agreements;

3. Update and provide training on confidentiality and security policies to all employees at least annually;

4. Train human resources, risk management, and other appropriate personnel on prompt and thorough investigation, and handling of suspected unauthorized disclosure, misappropriation, and misuse of

protected information;

5. Evaluate the investigation and handling of any incidents to identify the root cause of any issues and actions needed to prevent or minimize the opportunity for recurrence;

6. Monitor password protocol compliance, including employee practices for storing passwords (*i.e.,* such as the use of password management software as opposed to sticky notes or personal cell phones);

7. Work with counsel to update all personnel policies and workplace rules relating to technology usage and protecting confidential information;

8. Verify that limitations on the access to protected information are being observed, that only those individuals who need access have it, and that effective technology is in place to lawfully monitor and record who accesses and uses confidential information and trade secrets;

9. Verify that confidential information and trade secret information is marked confidential, proprietary, or trade secret, as applicable, and handled properly and carefully, *i.e.*, not being displayed on computers without screen savers in view of those who do not need access and not being left uncovered on desks when an office is unattended and unsecured; and

10. Verify that employee departure and onboarding protocols are developed, documented, and followed.

Trust without verification is merely a hope or a wish as one company recently learned when its request for a preliminary injunction in a trade secrets case was denied. In *Freedom Capital Group LLC v. Blue Metric Group, LLC,* Freedom Capital requested an injunction under federal and state trade secret laws to prevent misappropriation by its former outside counsel and an independent contractor. Freedom Capital asserted that it took reasonable steps to keep its trade secrets and confidential information, including secure access credentials and training representatives on confidentiality rules. The court found, however, that Freedom Capital gave independent contractors access to purportedly sensitive information without any confidentiality or non-disclosure agreements. The court also rejected Freedom's assertion that it trained its representatives on confidentiality obligations because it failed to produce any evidence of relevant training materials or communications.

This case illustrates the need to have a plan for securing your protected information and regularly auditing the efficacy of that plan. Verifying that the protection plan is working will place your company in a strong position to prevent and, if necessary, successfully pursue legal relief in the event of disclosure, misappropriation, and misuse of your confidential information and trade secrets.

Baker Donelson continues to monitor the developments associated with the FTC's rule banning non-competes, which remains set to take effect on September 4. We will be issuing future alerts related to the steps that companies should consider taking to protect their competitive edge. Our next alert will focus on specific steps and protocols companies can take regarding both their agreements and several of the steps above, including physical security and employee protocols. Look for additional webinar details in our next alert, formal event invitation to follow. If you have any questions, please contact a member of Baker Donelson's Labor & Employment or Intellectual Property teams.