FELICELLO

# Protecting Your Business: Practical Tips To Keep Your Trade Secrets Secret

Everyone is talking about the new rule approved by the Federal Trade Commission on April 23 (published[1] on May 7 and set to take effect – pending legal challenges[2] – on September 4, 2024[3]). It is referred to as the Non-Compete Clause Rule. The Non-Compete Clause Rule follows on the heels of several states effectively "outlawing" non-competition agreements. It prohibits, as "an unfair method of competition," all non-competition clauses or agreements between workers and employers as of the effective date. Many fear that this rule means the end of protecting a company's trade secrets. It does not.

Many companies that enter into non-competition agreements are not trying to keep employees from working, but rather trying to maintain the confidentiality of their trade secrets. They want to prevent other companies from obtaining, or their employees from using, their special sauce that sets the company apart from its competitors. Protecting trade secrets – the secret sauce – is a legitimate business goal. That goal can be achieved[4] without non-competition agreements that may (now) run afoul of various state and federal rules. Here are some practical tips to protect your trade secrets:

1. **IDENTIFY** – What are your trade secrets?

You need to know what your company's trade secrets are so that you can protect them. That means understanding what makes your business distinct, what gives it a competitive advantage, and what can be legally protected as a "trade secret."

If your business hasn't undertaken this exercise before, it's a useful annual exercise to review at the senior management and board level. If this is your first time – or you need a refresher, these two steps are useful. First, have your core businesspeople identify what information is most important to how they do their jobs and bring value to the company. This could include customer lists,[5] pricing information,[6] manufacturing designs and processes,[7] or intellectual property. Second, work with your attorney to compare those confidential secrets with what is legally protectable by trade secrets law. That analysis includes questions around two main ideas: Is your information public? Is your information valuable? [8]

Is your information public?

(1) Is the information known outside of your business?

(2) Is the information known by employees, contractors, and business partners?

Is your information valuable?

(3) What measures does your company take to guard the secrecy of the information?

(4) What is the value of the information to your company and your competitors?

(5) How much effort or money has your company spent to develop the information?

(6) How easy would it be for another company to duplicate or acquire the information?

1. **PROTECT, EDUCATE, AND MONITOR** – Leverage your internal resources.

So, now you know what your trade secrets are. Great! The next step is to take reasonable measures to protect your trade secrets. Initially, you want to put in place electronic, physical, and conceptual protections to keep your trade secrets secret. And, reasonable measures are required in order to obtain any type of legal relief – you can't just say, "it's a trade secret," and expect a court to agree. You've educated your people, so now it's time to use them and your company's resources to protect your secrets. You can use your HR team, IT team, legal team, and your sales/deals team.

Protections fall into two categories: external and internal. External include requiring non-disclosure or confidentiality agreements (NDAs) for any sharing of confidential, proprietary, or trade secret information. Tap into your sales and deals teams so that they reach out to your legal team to prepare appropriate agreements. NDAs provide some protection for your trade secrets and their breach can support claims that your company could bring under state and federal law.

Internal protection starts with educating your workforce about why your trade secrets are important. Your employees are the gatekeepers for your trade secrets. You need to educate your employees (and contractors if you use them) about the importance of safeguarding your company's special sauce. They need to understand what types of information your company treats as trade secrets, the consequences of disclosing them to unauthorized individuals, and that your company takes protection seriously. Annual reminders and trainings will help establish your company's culture of protection. Training for new employees and contractors is also important, as

are confidentiality agreements[9] for each new hire. Encourage your employees to be active participants in protecting your trade secrets.

Internal protection and monitoring includes adding protections to files and documents that prevent their download or external emailing; view access only for highly sensitive materials; remote access/wipe permission if you allow employees to use their own devices for work; monitoring employee email/downloads; limiting access to employees who need to know the information; requiring passwords and encryption to protect electronic trade secrets; keycard access, security cameras, physical locks; and cyber security monitoring/protections. These measures require the support of your IT, HR, and security teams.

Another branch of internal protection and monitoring comes into play when bringing on new employees or when employees are leaving. Hiring managers and HR should be aware of these protections and help. For incoming (new) employees, you should confirm with them that they are not bringing any trade secrets from their prior employers. New employees can be required to reimburse the company for training if they leave within a short period. For outgoing/departing employees, you should remind them that they are not permitted to take company information with them (and possibly have in place a computer policy that prevents them from downloading or emailing documents) and obtain permission to take any personal information that may be stored on a company device (such as photos or personal documents) before departure. A team comprised of representatives from legal, business, and HR should also consider whether the departing employee has had access to trades secrets that will “inevitably” be sued in her or his new employment to provide a substantial advantage to a competitor.[10] Garden leave (a paid period before beginning a new job)[11] and severance pay may be considered as protectionary measures for senior employees with access to particularly sensitive information. If garden leave is part of an employee’s departure, HR and legal should review with the employee the terms of that leave. Departing employees should ideally sign a confirmation that they have not taken any trade secrets upon departure and have returned any information obtained during their employment; incoming employees should ideally sign a confirmation that they are not bringing someone else’s trade secrets with them. The same procedures can be followed for consultants.

A final aspect of protecting and monitoring is a combination of internal and external, focused on your relationships with external business partners. This is your sales and deals teams together with your legal team. By understanding the scope of the deal or project, you can limit the information shared to the minimum information required for that purpose. At the end of every project or business relationship, and whenever a project or relationship changes, materials should be returned/destroyed (with appropriate confirmations), continued access should be confirmed and/or taken away, and records should be made of who had access to what information and when that access was removed.

1. **CHECK-UP** –Do your current policies and procedures protect your trade secrets?

Regularly review your trade secret protection policies. As your business grows, you may need to update your trade secret protection policies to ensure that they are still effective and protect what needs to be protected. Good corporate hygiene includes an annual check-up of your company's policies, procedures, and agreements,[12] as well as check-ups when something significant occurs (for example, a new process is created, a new patent is filed, or a new contract is won). Significant events might require adding to the information considered trade secrets and how that information is protected. Annually you should also check on who has access to what information (see discussion in point 2) and which employees, contractors, or business partners no longer should have access to sensitive information.

1. **PLAN AHEAD** – What happens if the worst happens?

Have a plan of action for what to do if your trade secrets are stolen or misused. You will want to act fast if you learn of the misuse of your trade secrets or if you suspect that they are being misused. In creating your plan, you should include your lawyer, IT, and HR. Legal options can include written demands for return of trade secrets, restraining orders obtained from a court, and state[13] and federal[14] litigation for damages (compensatory and punitive) resulting from the misuse and/or theft of trade secrets. You will also want to preserve records related to your trade secrets, including measures you took to protect the secrets, when/where/how the misappropriating party obtained secrets, and when/where/how you learned of the theft, misuse, and/or misappropriation of your trade secrets. This often involves IT obtaining email or download logs and security checking entry/access logs. Having a plan in place before anything happens can increase the chances of a positive outcome and the protection of your trade secrets.

[1] Federal Register, 89 FR 38342, available at https://www.federalregister.gov/d/2024-09171.

[2] See Ryan LLC v. Fed. Trade Commission, Civ. Action No. 3:24-CV-00986-E (N.D. Tex. April 24, 2024); Chamber of Commerce of the U.S.A. v. Fed. Trade Commission, Case No. 6:24-cv-00148 (E.D. Tex. April 24, 2024); ATS Tree Servs., LLC v. Fed. Trade Commission, No. 2:24-cv-1743 (E.D. Pa. April 25, 2024).

[3] The U.S. Chamber of Commerce filed a motion to stay the effective date of the Non-Compete Clause Rule pending final determination of the legal challenge. Ryan LLC v. Fed. Trade Commission, Doc. 47, Civ. Action No. 3:24-CV-00986-E (N.D. Tex. May 10, 2024).

[4] The FTC recognized that alternatives to non-competes for the "protection of trade secrets and other confidential information" include "enforcement of

intellectual property rights under trade secret and patent law, NDAs, and invention assignment agreements, … fixed duration contracts [for employees], and competing on the merits to retain workers by providing better pay and working conditions." Federal Register, 89 FR 38424.

[5] N. Atl. Instruments, Inc. v. Haber, 188 F.3d 38, 44 (2d Cir. 1999) (customer lists are protectible as trade secrets when the "list [is] developed by a business through substantial effort and kept in confidence[,] ... provided the information it contains is not otherwise readily ascertainable").

[6] Jasco Tools, Inc. v. Dana Corp. (In re Dana Corp.), 574 F.3d 129, 152 (2d Cir. 2009) ("Confidential proprietary data relating to pricing, costs, systems, and methods are protected by trade secret law").

[7] Faiveley Transp. Malmo AB v. Wabtec Corp., 559 F.3d 110, 117 (2d Cir. 2009) ("manufacturing drawings pertaining to dimensions and tolerances, surface finishes, material selection and treatments, lubrication specifications, and special instructions for manufacture, testing, and assembly, contain trade secrets").

[8] Unisource Worldwide, Inc. v. Valenti, 196 F. Supp. 2d 269, 278 (E.D.N.Y. 2022) (quoting Softel, Inc. v. Dragon Med. & Scientific Communications, Inc., 118 F.3d 955, 968 (2d Cir. 1997), cert. denied, 523 U.S. 1020 (1998) and N. Atl. Instruments, Inc. v. Haber, 188 F.3d 38, 44 (2d Cir. 1999)). These factors were first enumerated in Ashland Management, Inc. v. Janien, 82 N.Y.2d 395, 407 (1993) (quoting Restatement of Torts § 757, cmt. b).

[9] Ensure that employee confidentiality agreements comply with the notice provisions of 18 U.S.C. §1833 to preserve the ability to obtain punitive damages and attorneys' fees.

[10] This is sometimes referred to as the "inevitable disclosure" doctrine and, in certain situations, courts can grant injunctive relief preventing a departing employee from starting a new job with a competitor. E.g., PepsiCo, Inc. v. Redmond, 54 F.3d 1262, 1270-71 (7th Cir. 1995) (granting injunction where "PepsiCo has asserted that Redmond cannot help but rely on PCNA trade secrets as he helps plot Gatorade and Snapple's new course, and that these secrets will enable Quaker to achieve a substantial advantage by knowing exactly how PCNA will price, distribute, and market its sports drinks and new age drinks and being able to respond strategically"); but see, e.g., Sunbelt Rentals, Inc. v. McAndrews, 552 F. Supp. 3d 319, 330-32 (D. Conn. 2021) (denying injunction given "the disfavored nature of the inevitable disclosure doctrine, the absence of a high degree of similarity between Defendant's old and current positions, and the somewhat dissimilar relationships with customers of Sunbelt and Riggs Distler in providing matting services").

[11] Garden leave should also be reviewed. It is often considered as compensation for a period of non-competition. You should consult with your

lawyer about whether new garden leave may be affected by the Non-Compete Clause Rule.

[12] If/when the Non-Compete Clause Rule goes into effect, it requires notification to all employees who are currently covered by a non-compete, telling them that the non-compete is no longer enforceable. See Non-Compete Clause Rule, 16 CFR §910.2(b). The annual contract review can assist in compliance with the rule's requirements.

[13] State law claims might include trade secret misappropriation, breach of contract, and business torts. Almost every state in the U.S., plus D.C. and the U.S. Virgin Islands, have enacted a version of the Uniform Trade Secrets Act (exceptions are New York, where it was recently introduced in the 2024 legislative session, and North Carolina). See Uniform Law Commission, Trade Secrets Act, Bill List, available at https://www.uniformlaws.org/committees/community-home?communitykey=3a2538fb-e030-4e2d-a9e2-90373dc05792. The Uniform Trade Secrets Act provides for attorneys' fees, in addition to compensatory and punitive damages. The common law also provides for protection of trade secrets and other torts that can provide relief, but not access to attorneys' fees.

[14] The federal Defend Trade Secrets Act, 18 U.S.C. §1836, provides a private cause of action for theft of trade secrets, and Economic Espionage Act, 18 U.S.C. §1832 et seq., provides for criminal penalties, including fines, forfeiture, and imprisonment.