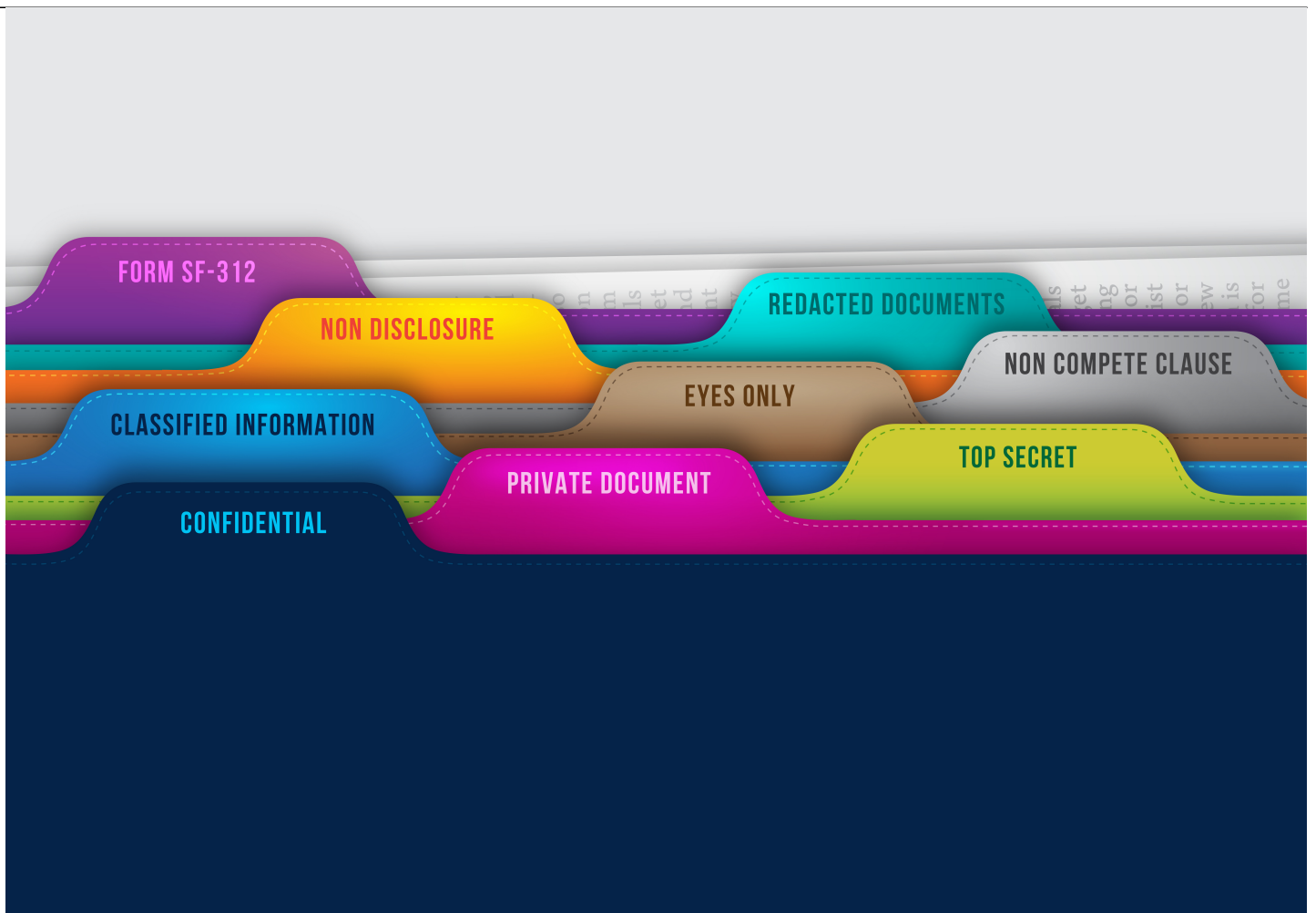




Protect Your Company with These 4 Steps While the Future of Noncompetes is Decided

Commercial and Contracts

Employment and Labor



Banner artwork by acarapi / *Shutterstock.com*

Noncompete agreements may soon become a contract clause of the past if the US Federal Trade Commission (FTC) survives the legal challenges filed in federal court banning them.

The FTC Rule, issued April 23, 2004, will reshape how companies handle attrition (voluntary and involuntary), as well as hiring policies. Meanwhile, employers also contend with a patchwork of state law that limits or bans noncompetes. This confluence of events is an inflection point for in-house counsel, who can take four proactive steps to protect their company's interests.

The FTC rule and related litigation

To briefly summarize, the FTC Rule, if implemented, will ban noncompete agreements between employers and workers starting as early as September 4, 2024. The definition of worker includes employees, independent contractors, volunteers, interns, and externs. Employers will be required to notify employees by hand, mail, email, or text.

The FTC Rule includes two narrow exceptions to the ban on noncompete:

-
- Senior executives who are currently subject to noncompete, earn more than US\$151,164 per year, and have policymaking authority — that is, final authority to make policy decisions that control significant aspects of a business entity or common enterprise.
 - Noncompete agreements are and will continue to be valid when there is a bona fide sale of the business, of the person's ownership interest in a business entity, or all or substantially all of a business entity's operating assets.

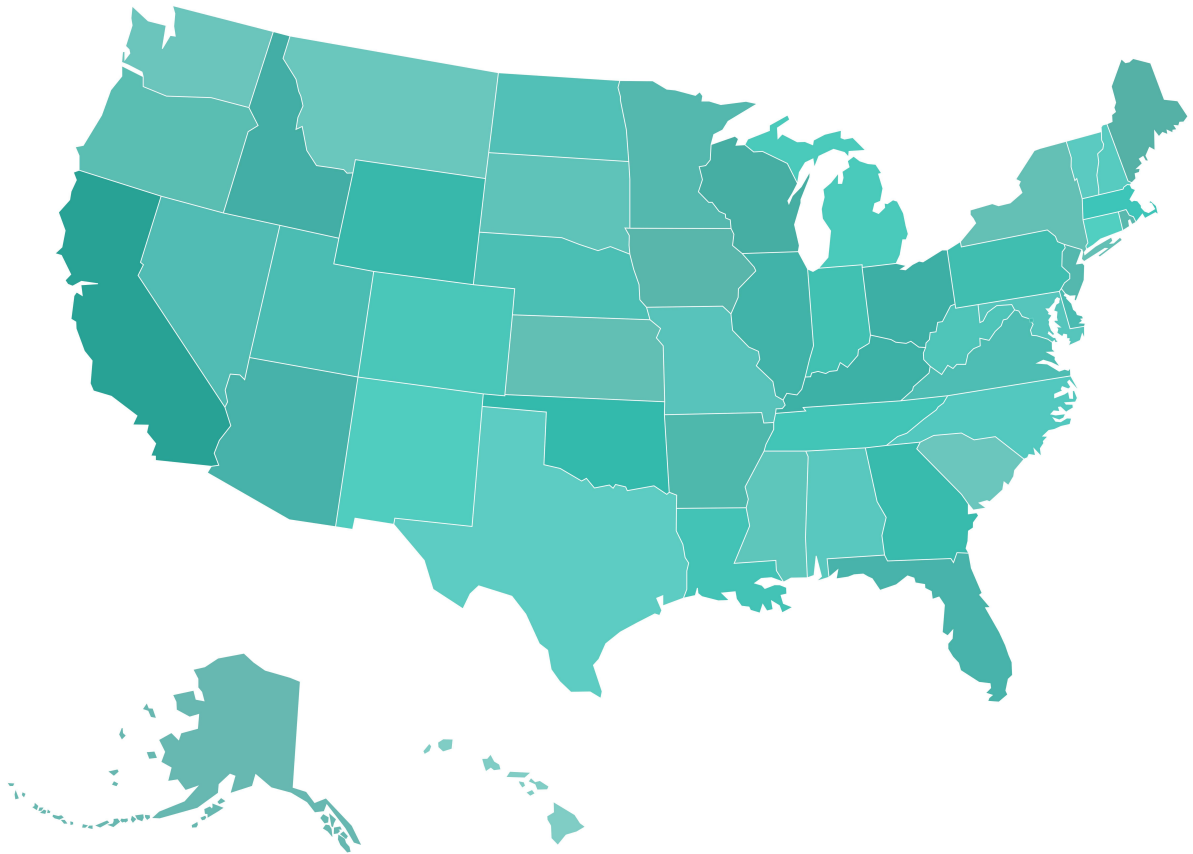
Three lawsuits have been filed in federal court to enjoin the FTC Rule before it takes effect. The crux of these lawsuits is that noncompete agreements are acceptable methods of competition under Section 5 of the FTC Act and the FTC lacks authority to regulate them. The first ruling on the merits in these cases, *Ryan LLC v FTC*, is expected by 2024. At least one of these lawsuits is likely to reach the US Supreme Court.

State law trends

Before the FTC Rule was issued, several states enacted legislation restricting noncompetes. Four states (California, Minnesota, North Dakota, and Oklahoma) have banned them entirely with narrow exceptions. Six states (Illinois, Maine, Massachusetts, Michigan, Rhode Island, and Wisconsin) and New York City have pending legislation that, if enacted as written, would also ban employee noncompete agreements.

Ten states and the District of Columbia prohibit noncompetes for workers at or below specified salary thresholds. In states that have not enacted noncompete statutes, case precedent determines what constitutes an enforceable agreement although the criteria vary across jurisdictions.

-



Noncompete trends and regulations have varied across many different states over time. Pyty / Shutterstock.com

4 proactive steps to protect the company

While the FTC Rule winds through the courts, and as more states enact their own noncompete statutes, this is an opportune time for in-house counsel to take an inventory of documents, data, and employment policies to protect competitively sensitive information.

1. Find the documents.

The impact of the FTC Rule and state legislation extends beyond employment agreements and offer letters and so should an in-house audit of potentially relevant documents. Noncompetes — and clauses that create de facto noncompetes — may be found in handbooks and policy documents, equity grants, intellectual property licenses, and legacy documents from prior mergers and acquisitions. These documents should be reviewed and revised on a periodic basis to keep pace with the changing regulatory landscape.

2. Secure the data.

Senior executives use competitively sensitive data to oversee business operations, but access should be narrowly tailored both within and outside the C-suite. In-house counsel should understand where competitively sensitive information is stored, such as file cabinets, servers, hard drives, and take measures to secure it through multi-factor authentication or a simple lock and key. Robust information technology (IT) systems are particularly effective in detecting potential breaches. Even though concerns about unauthorized downloads are heightened when a worker is leaving the company, misappropriation can occur at any time, even with workers who appear to be in good standing.

3. Protect the data with other provisions.

The potential death knell of noncompetes does not leave employers without recourse if a former worker goes rogue. Non-disclosure, limited use, and non-solicitation clauses also discourage misuse of company data. But to be effective, post-employment obligations and penalties for violations must be clearly stated in the relevant contracts, among other requirements, to ensure they are enforceable.

4. Caution against “self-help” and other pitfalls.

Well-defined employment policies and documents protect the company and individuals from civil and criminal liability. Hiring and onboarding procedures should thoroughly vet and train new workers to minimize the risk that they may misuse their former employer’s proprietary information or otherwise violate post-employment confidentiality obligations. Equally important, human resource professionals and hiring managers should not make promises or reach understandings with other companies amounting to no-poach or wage-fixing agreements that violate US antitrust law. The Department of Justice, Antitrust Division routinely prosecutes companies and individuals who engage in this misconduct.

Whatever the outcome, find a way to safeguard company interests

Whether or not the FTC Rule takes effect in September, this is an opportune time for in-house counsel to ensure that no matter what the legal landscape, the company’s competitively sensitive information is protected when a worker leaves. Fortunately, noncompete agreements are not the only way to safeguard company interests. In-house counsel can take these four simple steps to manage the documents, data, and employment policies and mitigate risk at all stages of the employee lifecycle.

[Join ACC](#)

Disclaimer: The information in any resource in this website should not be construed as legal advice or as a legal opinion on specific facts, and should not be considered representing the views of its authors, its sponsors, and/or ACC. These resources are not intended as a definitive statement on the subject addressed. Rather, they are intended to serve as a tool providing practical guidance and references for the busy in-house practitioner and other readers.

[Jennifer M. Driscoll](#)



Counsel and Co-Chair of Antitrust and Trade Regulation Group

Robinson+Cole

Jennifer M. Driscoll is counsel and co-chair of the Antitrust and Trade Regulation Group at Robinson+Cole. Her practice focuses on antitrust counseling, litigation, investigations, and mergers. She is also a certified information privacy professional in the US and EU and works on cybersecurity investigations.

[Michaelynn Ware](#)



Vice President, Legal Operations and Intellectual Property

Otis Elevator Company

Michaelynn Ware most recently served as vice president, legal operations and intellectual property at Otis Elevator Company. She started her legal career as an antitrust lawyer at Hogan Lovells in Washington, DC. Since that time, she has held a variety of senior in house positions, including serving as the chief antitrust counsel at the former United Technologies Corporation, VP & Counsel for Pratt & Whitney's Commercial Engines division, and General Counsel for Otis in the Asia Pacific region, based in Singapore.

[Abby M. Warren](#)



Partner

Robinson+Cole

Abby M. Warren is a partner in Robinson+Cole's Labor and Employment Group, where she focuses her practice on counseling private sector employers, including multinational corporations, health care organizations, educational institutions, and manufacturers, in all areas of employment law including litigation and investigations.

