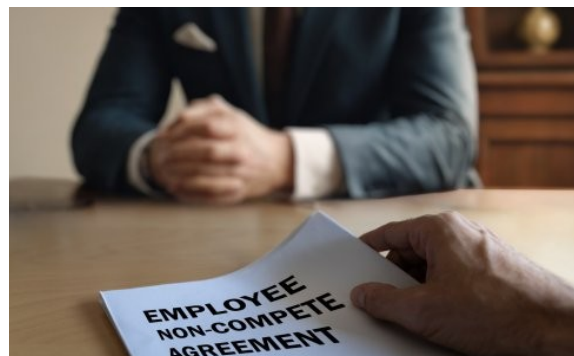


Safeguarding Your Business in an Era of Restrictive Covenant Scrutiny

February 27, 2026
By Patrick Duffey



For years, businesses have relied on non-competes and broad confidentiality agreements to protect themselves when employees leave. That approach is changing. Courts and regulators are increasingly wary of restrictions that limit employee mobility, as reflected in the last several years of activity by the Federal Trade Commission, the National Labor Relations Board, and state legislatures.

This shift, however, is not anti-business. It is aimed at curbing overbroad restraints that prevent former employees from earning a living. In many respects, it reflects a return to the true purpose of restrictive covenants: protecting legitimate business interests and competitive advantage. As a result, employers' litigation focus is moving away from preventing former employees from simply joining competitors and toward examining whether company information was improperly taken or used. In practical terms, protecting the business now centers on protecting its data.

Importantly, restrictive covenants are not dead. Properly tailored covenants remain enforceable in most jurisdictions and continue to play a meaningful role in safeguarding legitimate interests. Courts are far more likely to enforce restrictions that are narrowly drafted, periodically reviewed, and tied to an employee's role and access to sensitive information. Employers should therefore refine—not abandon—restrictive covenants to ensure they can withstand scrutiny. Within this framework, data protection operates as a supplement to, not a replacement for, other restrictive covenants, providing an added safeguard if contractual restrictions are narrowed or fail.

Most businesses are not harmed simply because a former employee takes a new job. Rather, the harm occurs when something leaves with that employee: customer lists, pricing strategies, internal processes, technical know-how, reports, or analytics. To qualify for protection, this information must be valuable, not generally known, and subject to reasonable safeguards. Modern disputes increasingly turn on trade secret principles under the Defend Trade Secrets Act and comparable state laws. Courts focus less on contractual labels and more on whether the company actually treated the information as valuable.

Effective protection requires more than labeling information "confidential." At hiring, employees should be clearly informed about the information they will access and the limits on its use. At departure, employers should require exit certifications confirming that devices were returned, company files were removed from personal accounts, and no information was retained or forwarded. This process alone prevents many disputes and creates a clear record if concerns later arise, allowing employers to investigate based on objective representations rather than speculation.

During employment, employers increasingly rely on monitoring tools that provide objective evidence of whether files were accessed, transferred, or retained improperly. Courts are generally more receptive to such technical proof than to assumptions based solely on an employee joining a competitor.

The takeaway is straightforward. Courts are becoming less concerned with where a former employee works and far more concerned with whether protected information was misused. Businesses best positioned going forward will not be those with the longest non-compete agreements, but those that can show they identified their critical information and consistently safeguarded it.