GRAND PARK LAW GROUP
A PROFESSIONAL CORPORATION

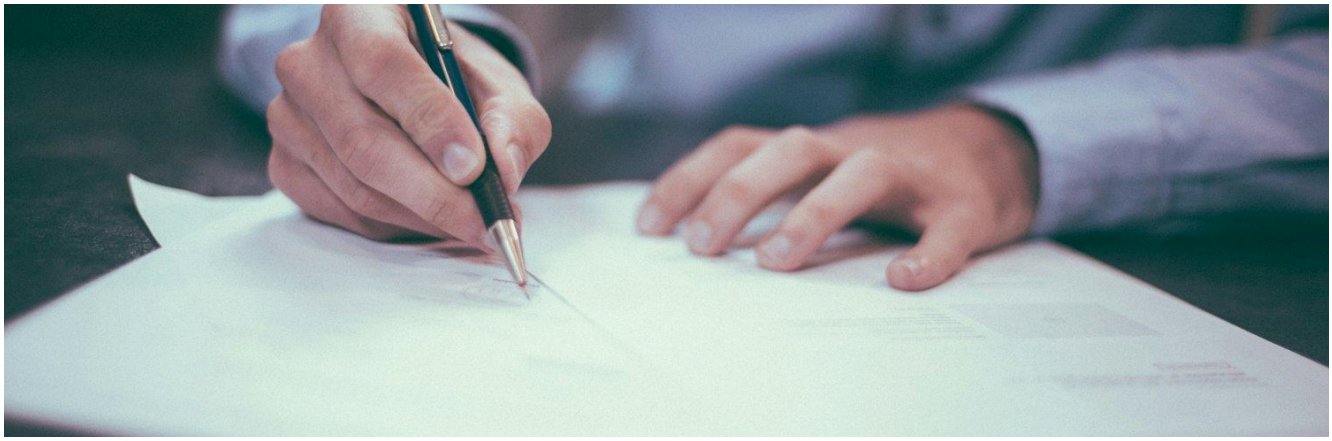
WESTSIDE TOWERS
11835 W. Olympic Boulevard #870E
Los Angeles, California 90064

O:+1 888.629.4754
F: +1 310.900.0805

PRACTICE BRIEF · BUSINESS TORTS

Business Torts: Recent Developments 2024-2025 — Trade Secrets, Non-Solicitation, and Emerging Digital Claims

Grand Park Law Group · August 2025 · 15 min read



In This Article

1. I. AMN Healthcare and the End of Non-Solicitation Agreements
2. II. CUTSA Preemption: Clarifying the Boundaries
3. III. Trade Secret Valuations in Technology Disputes
4. IV. Unfair Competition in the Cannabis Industry
5. V. AI and Confidential Information Misappropriation

The 2024-2025 period has produced several consequential developments in California business tort law. From the continued fallout of *AMN Healthcare* and the legislative codification of California's broad anti-restraint-of-trade principles, to emerging questions about AI systems and trade secret misappropriation, the landscape has shifted in ways that affect how companies structure employment relationships, protect proprietary information, and litigate commercial disputes. This article surveys five major developments and their practical implications for businesses operating in California.

I. AMN Healthcare and the End of Non-Solicitation Agreements

California has long been the most employee-friendly jurisdiction in the nation with respect to post-employment restrictive covenants. Business and Professions Code section 16600 provides, with narrow statutory exceptions, that "every contract by which anyone is restrained from engaging in a lawful profession, trade, or business of any kind is to that extent void." In *Edwards v. Arthur Andersen, LLP*, 44 Cal.4th 937 (2008), the California Supreme Court rejected the Ninth Circuit's "narrow restraint" exception and held that section 16600 must be read broadly: any contractual restraint on a former employee's professional activities is void unless it falls within one of the statute's express exceptions (sale of a business, dissolution of a partnership, or dissolution of an LLC).

The question left open by *Edwards* was whether this prohibition extended to customer non-solicitation agreements — provisions that do not prohibit an employee from working for a competitor but do prohibit the employee from soliciting the former employer's clients. In *AMN Healthcare, Inc. v. Aya Healthcare Services, Inc.*, 28 Cal.App.5th 923 (2018), the California Court of Appeal answered that question definitively: customer non-solicitation provisions are restraints of trade under section 16600 and are void. The court reasoned that a prohibition on soliciting clients effectively restrains the employee from fully engaging in the profession, because client relationships are a core component of professional activity in industries such as healthcare staffing, consulting, and financial services.

The practical reverberations of *AMN Healthcare* continued through 2024-2025 in two significant ways. First, AB 1076, which took effect on January 1, 2024, codified the broad interpretation of section 16600 by adding subdivision (b): "an employer, or a person acting on behalf of the employer, shall not enter into or attempt to enforce a noncompete agreement, regardless of where or when the agreement was signed." The statute further requires employers to notify current and former employees that any noncompete provisions in their agreements are void. Second, the enactment of SB 699 in 2024 extended these protections extraterritorially, providing that a noncompete agreement is void regardless of where and when it was signed, and creating a private right of action for employees subjected to enforcement of void agreements.

For staffing agencies, professional services firms, and technology companies, the combined effect of *AMN Healthcare*, AB 1076, and SB 699 is that virtually no post-employment restrictive covenant — whether styled as a non-compete, non-solicitation, or no-hire provision — is enforceable in California. The only viable contractual mechanism for protecting client relationships is a well-drafted trade secret agreement that protects genuinely confidential information without restricting the employee's right to compete.

II. CUTSA Preemption: Clarifying the Boundaries

The California Uniform Trade Secrets Act (Civil Code sections 3426-3426.11) provides the exclusive statutory framework for trade secret misappropriation claims in California. Section 3426.7 expressly preempts other civil remedies "based upon misappropriation of a trade secret,"

| Beverly Hills • San Francisco • San Diego • Chicago |
| Main: (888) 629-GPLG (4754) • Fax: (310) 900-0805 • www.GrandParkLawGroup.com |

and the scope of that preemption has been one of the most actively litigated issues in California business tort practice.

The foundational case remains *Silvaco Data Systems v. Intel Corp.*, 184 Cal.App.4th 210 (2010), which established the "gravamen" test: a common-law or statutory claim is preempted if the nucleus of facts necessary to prove the claim is the same as the nucleus of facts necessary to prove trade secret misappropriation. Under *Silvaco*, the preemption inquiry does not turn on how the plaintiff labels the claim. It turns on whether the wrongfulness of the defendant's conduct depends on the information being a trade secret. If the claim can succeed only by proving that the defendant took or used a trade secret, it is preempted — regardless of whether it is captioned as conversion, breach of confidence, unjust enrichment, or unfair competition.

Developments in 2024-2025 have further refined the boundaries of what survives CUTSA preemption and what does not. Four categories of claims have emerged with increasing clarity:

Breach of contract claims survive preemption. A claim for breach of a nondisclosure agreement, confidentiality provision, or employment agreement is grounded in the contractual obligation, not in trade secret law. The wrongfulness of the breach flows from the promise itself, and the claim can be established even if the information disclosed does not meet CUTSA's statutory definition of a trade secret. This makes breach of contract the most reliable parallel cause of action in trade secret litigation.

Breach of fiduciary duty claims survive when the duty is independent. An officer or director who diverts corporate opportunities, engages in self-dealing, or uses company resources for personal benefit can be sued for breach of fiduciary duty even when the same conduct involves trade secret misappropriation. The key is that the fiduciary breach must be independently wrongful — the claim must not depend on proving that the information at issue qualifies as a trade secret.

UCL section 17200 claims face a mixed outcome. An unfair competition claim under Business and Professions Code section 17200 survives preemption where the predicate unlawful, unfair, or fraudulent act is something other than the misappropriation itself — for example, a violation of the Computer Fraud and Abuse Act or a breach of contract. But where the only unlawful conduct alleged is the trade secret misappropriation, the UCL claim is preempted because it is entirely derivative of the CUTSA theory.

Fraud claims survive when the misrepresentation is the gravamen. A claim based on affirmative misrepresentation — for example, a defendant who induced disclosure by falsely representing the purpose for which confidential information would be used — survives preemption because the wrongful act is the fraud, not the use of a trade secret. By contrast, a claim that is styled as fraud but whose real gravamen is the unauthorized use of proprietary information will be preempted.

For practitioners, the lesson of 2024-2025 is that pleading strategy matters enormously in trade secret cases. Plaintiffs who allege only misappropriation-based claims risk losing every cause of action except the CUTSA claim on a preemption motion. The better approach is to plead parallel

claims with independent factual bases and to articulate clearly, in the complaint itself, why each non-CUTSA claim does not depend on trade secret status.

III. Trade Secret Valuations in Technology Disputes

Establishing the value of misappropriated trade secrets is among the most difficult evidentiary challenges in business tort litigation. CUTSA provides for three measures of damages: the plaintiff's actual loss, the defendant's unjust enrichment (to the extent not accounted for in the actual loss calculation), and a reasonable royalty (Civil Code section 3426.3). The federal Defend Trade Secrets Act (18 U.S.C. section 1836) provides substantially identical remedies. In practice, these three theories require very different types of expert analysis, and the 2024-2025 period has seen increased judicial scrutiny of the methodologies that experts use to calculate each measure.

The reasonable royalty approach asks what a willing licensor and willing licensee would have agreed to in a hypothetical negotiation at the time the misappropriation occurred. This methodology, borrowed from patent damages law, requires the expert to construct a hypothetical negotiation scenario that accounts for the value of the trade secret to the defendant's business, the availability of non-infringing alternatives, and the competitive advantage conferred by the secret. Courts in 2024-2025 have scrutinized whether experts adequately tie their royalty rates to the specific trade secret at issue, rather than to the plaintiff's broader technology portfolio.

The unjust enrichment measure focuses on the benefit the defendant derived from the misappropriation. In technology cases, this often requires attributing a portion of the defendant's revenue or profits to the misappropriated trade secret — an exercise that becomes extraordinarily complex when the secret is one input among many in a multi-component product. The apportionment problem is particularly acute for algorithmic trade secrets and proprietary datasets, where the trade secret's contribution to the defendant's product may be real but difficult to quantify in isolation.

The avoided-costs methodology measures damages by the research and development expenditures that the defendant avoided by misappropriating the plaintiff's trade secret rather than developing the technology independently. This approach has gained traction in software disputes, where the cost of engineering a competing solution from scratch is often well-documented. However, courts have required that the avoided-cost calculation account for the defendant's own pre-existing knowledge and the availability of public-domain alternatives.

Expert testimony on trade secret valuation must survive scrutiny under *Sargon Enterprises, Inc. v. University of Southern California*, 55 Cal.4th 747 (2012), which gives trial courts a gatekeeping role to exclude expert opinion that is based on speculation, conjecture, or assumptions that lack evidentiary foundation. In 2024-2025, several trial courts have excluded trade secret damages opinions where the expert failed to account for the portion of the defendant's product value attributable to non-trade-secret inputs, or where the expert relied on the plaintiff's total R&D investment without disaggregating the costs attributable to the specific trade secret at issue.

| Beverly Hills • San Francisco • San Diego • Chicago |
| Main: (888) 629-GPLG (4754) • Fax: (310) 900-0805 • www.GrandParkLawGroup.com |

The valuation of algorithmic trade secrets and proprietary datasets presents additional challenges. An algorithm's value often lies not in the code itself but in the training data, the iterative refinement process, and the competitive intelligence embedded in the model's outputs. Establishing what a "willing licensee" would pay for such a trade secret requires the expert to grapple with questions that have no clear precedent: How do you value a machine learning model that was trained on misappropriated data? What is the unjust enrichment when the defendant used the plaintiff's proprietary dataset to accelerate its own model development by months rather than producing a directly competing product?

IV. Unfair Competition in the Cannabis Industry

California's legal cannabis market, now generating billions in annual revenue, has produced a growing body of business tort litigation between competing operators. These disputes present unique legal challenges that arise from the tension between state legality and federal illegality.

Unfair competition claims under Business and Professions Code section 17200 have become a primary vehicle for cannabis operators to challenge competitors' business practices. The UCL's broad standing provisions and its three independent prongs — unlawful, unfair, and fraudulent — provide multiple theories of liability. Cannabis companies have brought UCL claims alleging that competitors operate without required licenses, exceed permitted cultivation area, sell untested products, or engage in deceptive marketing. Courts have generally permitted these claims to proceed on the theory that state-law unfair competition doctrine applies fully to businesses operating within California's regulatory framework, regardless of the federal status of the underlying product.

Trade secret protection for cannabis businesses raises distinct questions. Cultivation methods, extraction processes, strain genetics, and proprietary formulations can qualify as trade secrets under CUTSA if they derive independent economic value from not being generally known and are subject to reasonable measures to maintain their secrecy. However, the reasonable-measures requirement is complicated by the regulatory transparency mandates that cannabis operators face: state and local licensing authorities may require disclosure of cultivation practices, testing results, and product formulations as a condition of licensure. The extent to which compelled regulatory disclosure undermines trade secret protection remains unsettled.

The most significant doctrinal issue in cannabis business tort litigation is the federal illegality defense. Defendants in cannabis disputes have argued that courts should refuse to adjudicate claims arising from a federally illegal enterprise, invoking the unclean hands doctrine and public policy. The California courts have largely rejected this defense. Following the reasoning in *Manzuri v. National Western Financial, Inc.* and related authorities, courts have held that California's comprehensive regulatory scheme for cannabis confers sufficient state-law legitimacy to support adjudication of business tort claims between licensed operators. The unclean hands defense has been held inapplicable where both parties are operating within California's regulatory framework, because neither party's "unclean hands" are any dirtier than the other's.

| Beverly Hills • San Francisco • San Diego • Chicago |
| Main: (888) 629-GPLG (4754) • Fax: (310) 900-0805 • www.GrandParkLawGroup.com |

The federal illegality defense retains some force in narrow circumstances. Federal courts remain reluctant to enforce contracts that require ongoing violations of the Controlled Substances Act, and the inability to obtain federal intellectual property protection (patents, trademarks) leaves cannabis operators more dependent on state trade secret law as their primary IP protection mechanism. For cannabis businesses, rigorous trade secret protocols — documented confidentiality agreements, restricted access controls, and careful management of regulatory disclosures — are essential precisely because federal IP protections are unavailable.

V. AI and Confidential Information Misappropriation

The rapid adoption of generative AI tools in the workplace has created a new category of trade secret risk that did not exist two years ago. When an employee inputs confidential business information into a third-party AI tool — whether a large language model, a code-generation assistant, or a data analysis platform — the legal consequences under both CUTSA and the Defend Trade Secrets Act are significant and largely untested.

The threshold question is whether inputting trade secret information into an AI system constitutes "misappropriation" under CUTSA. Section 3426.1(b) defines misappropriation to include disclosure or use of a trade secret by a person who knew or had reason to know that the trade secret was acquired through improper means, or in violation of a duty to maintain its secrecy. Where an employee feeds confidential information into a third-party AI tool in violation of a confidentiality agreement or company policy, the act of disclosure to the AI platform may itself constitute misappropriation. But the analysis becomes more complex when the employee uses the AI tool in good faith, without understanding that the information will be retained, used for model training, or potentially surfaced to other users.

The Samsung data leak incident in 2023 — in which Samsung engineers reportedly entered proprietary source code and internal meeting notes into ChatGPT — serves as a cautionary example. The incident raised the question of whether information that is entered into a widely-used AI platform retains its trade secret status. Under CUTSA, a trade secret must "derive independent economic value from not being generally known to the public" (Civil Code section 3426.1(d)). If confidential information entered into an AI tool becomes accessible to other users or is incorporated into the model's training data, the information may lose its trade secret status entirely — not because the owner failed to value it, but because the AI platform's architecture made the disclosure effectively public.

The "reasonable measures" requirement presents the most immediate practical challenge. CUTSA requires that the trade secret owner take "efforts that are reasonable under the circumstances to maintain its secrecy" (Civil Code section 3426.1(d)). In the pre-AI era, reasonable measures typically included confidentiality agreements, access controls, document-marking protocols, and exit-interview procedures. In the AI era, reasonable measures must also address the risk that employees will input confidential information into AI tools. Companies that fail to implement AI-specific trade secret protocols — such as policies prohibiting the use of external AI tools for

| Beverly Hills • San Francisco • San Diego • Chicago |
| Main: (888) 629-GPLG (4754) • Fax: (310) 900-0805 • www.GrandParkLawGroup.com |

processing confidential data, technical controls that block uploads to unapproved AI platforms, and employee training on the trade secret implications of AI use — risk a judicial finding that they did not take reasonable measures to maintain secrecy.

The Defend Trade Secrets Act (18 U.S.C. section 1836) provides a parallel federal cause of action for trade secret misappropriation, including the possibility of ex parte seizure orders in extraordinary circumstances. The DTSA's reasonable-measures requirement mirrors CUTSA's, and federal courts are likely to apply the same analysis regarding AI-related disclosures. For companies with trade secrets that have both state and federal value, the AI risk multiplies: a single unauthorized disclosure to an AI platform could jeopardize both CUTSA and DTSA protections simultaneously.

Looking ahead, the intersection of AI and trade secret law will likely produce litigation on several fronts: whether an AI company that trains its models on user-submitted data can be held liable for trade secret misappropriation; whether AI-generated outputs that incorporate or are derived from trade secret inputs constitute "use" of the trade secret; and whether the trade secret owner's failure to implement AI-specific protections constitutes a failure to take reasonable measures. These questions will define the next chapter of trade secret jurisprudence in California and nationally.

KEY TAKEAWAYS FOR 2024-2025

- Non-solicitation agreements are void in California under *AMN Healthcare* and the codification in AB 1076 and SB 699; companies must rely on trade secret protections rather than restrictive covenants to protect client relationships
- CUTSA preemption eliminates most common-law claims that depend on proving trade secret status, but breach of contract, independent fiduciary duty claims, and non-derivative UCL claims survive; pleading strategy at the complaint stage is dispositive
- Trade secret valuation in technology cases requires rigorous expert methodology that apportions value to the specific trade secret and survives *Sargon* gatekeeping scrutiny; algorithmic secrets and proprietary datasets present novel apportionment challenges
- Cannabis industry business tort claims are generally adjudicable in California courts despite federal illegality; the unclean hands defense has limited application where both parties operate under California's regulatory framework
- AI-related trade secret risks require immediate updates to corporate confidentiality protocols, including policies on external AI tool use, technical controls on data uploads, and employee training; failure to address AI risks may undermine the "reasonable measures" element of trade secret claims

---

Practice	Business Torts
Topics	Trade Secrets · Non-Solicitation · CUTSA · Artificial Intelligence
Publication	Annual Review · 2024-2025

Available online at www.grandparklawgroup.com/practices/business-torts/insights/articles/recent-developments-2024-2025. This publication is provided for general information and is not legal advice.
© 2026 Grand Park Law Group, A.P.C. Attorney Advertising.

| Beverly Hills • San Francisco • San Diego • Chicago |
| Main: (888) 629-GPLG (4754) • Fax: (310) 900-0805 • www.GrandParkLawGroup.com |