International Franchise Association
58th Annual Legal Symposium
May 18-19, 2026

2026 Judicial Update & Legal Trends

Harris J. Chernow
Reger Rizzo & Darnall LLP

Bradford J. Kelley
Littler Mendelson, P.C.

Jennifer Daskal
Venable, LLP

Dominic Hui
Ribeiro Hui

Table of Contents

International Franchise Association
58th Annual Legal Symposium
May 18-19, 2026

2026 Select Franchise Cases and Legal Trends Update

Harris J. Chernow
Reger Rizzo & Darnall LLP
Philadelphia, PA

I. Introduction[1]

The below cases and legal trends represent some of the latest legal developments that impact (some indirectly) the field of franchise law. This paper provides a focused review and analysis of certain recent case law and other legal events shaping the franchise and legal landscape. It highlights key judicial decisions legislative proceedings addressing issues such as contractual enforcement, choice of law, the use of generative AI, and statutory franchise protections. While there are plenty of other cases affecting the franchise world, this representation is purely a subjective selection of noteworthy cases and trends. By examining how courts are currently interpreting and applying these principles, this paper aims to identify some emerging trends and offer practical insights for franchisor and franchisee lawyers navigating an evolving legal environment.

II. Non-Compete Cases

A. *The Filta Group, Inc. v. LXU, Ltd.*, No. 25-cv-914, 2025 WL 3718465 (M.D. Fla. Dec. 23, 2025)

Synopsis

In this case concerning trademark infringement and non-competition covenants, the court discussed the enforcement of restrictive covenants against non-signatories to those agreements.

Factual Background

Franchisees LXU, Ltd. (LXU) and Ken Melick entered into a franchise agreement with Franchisor Filta Group, licensing LXU to operate a Filta brand mobile commercial kitchen cleaning service company in Ohio, Indiana, and Kentucky.[2] The franchise agreement contained, among other terms:

- A provision requiring the continuous operation of the business during the term of the agreement;
- A guarantee from the owner of LXU, guaranteeing its performance and adherence to the Franchise Agreement's non-competition and non-solicitation provisions;
- A requirement that the franchisee's employees were required to sign confidentiality and/or non-competition agreements;
- A prohibition against the franchisee providing financing, other assistance, or facilities to any business that competes with Filta; and

[1] The author would like to thank Brody L. Graham, associate with Reger Rizzo & Darnall, LLP, for his extensive and invaluable contribution to this paper.

[2] *Filta Grp., Inc. v. LXU, Ltd.*, No. 6:25-cv-914-PGB-NWH, 2025 LX 502495, at *1-2 (M.D. Fla. Dec. 23, 2025)

- A right to inspect the franchisee's business, including its books and records, vans, and Mobile Filtration Units, and could direct a franchisee to provide a list of its customers.[3]

On October 1, 2024, one of LXU's employees (Defendant Farrer) formed the entity Kitchen Kare Innovations (KKI) with the stated intent of providing ventilation hood cleaning services.[4] LXU's owner never asked the employee to sign a confidentiality agreement.[5] Leading up to May 16, 2025, LXU had 1) not complied with a request from Franchisor for a customer list; 2) failed to have employees sign confidentiality agreements; 3) performed work outside of its designated territory; and 4) denied the franchisor access to its books, records, and facilities.[6]

On May 16, 2025, without providing the franchisor prior notice, the franchisees unilaterally terminated the Franchise Agreement and sent a letter using the Filta Mark to every customer.[7] The letter provided that LXU would no longer provide fryer management services, and served as an introduction to KKI who would reach out shortly to offer the same services under the same terms as they previously received.[8] Essentially, Defendant Farrer and KKI served as a place holder to maintain customers while LXU and Defendant Melick found a way to circumvent the non-competition clause.[9] Ultimately, KKI retained 150 out of the 450 LXU customer accounts.[10]

Filta filed a preliminary injunction for its breach of restrictive covenant and trademark infringement claims.[11]

Court's Analysis

The court granted the preliminary injunction as to both Franchisor Plaintiff's claims.[12] To obtain a preliminary injunction, a plaintiff must show: (1) substantial likelihood of success on the merits; (2) irreparable injury will be suffered unless the injunction issues; (3) the threatened injury to the movant outweighs whatever damage the proposed injunction may cause the opposing party; and (4) if issued, the injunction would not be adverse to the public interest.[13]

---

[3] *Id.* at *2-3.
[4] *Id.* at *5.
[5] *Id.* at *4.
[6] *Id.* at *6.
[7] *Id.*
[8] *Id.*
[9] *Id.* at *9.
[10] *Id.*
[11] *Id.* at *10.
[12] *Id.*
[13] *Id.* at *9.

Trademark Infringement

1. *Filta is Substantially Likely to Succeed on the Merits of its Infringement-Based Claims*

The Lanham Act provides that a claim for trademark infringement is established when a trademark holder can demonstrate that the use of its trademark by another is likely to confuse consumers as to the source of the product."[14] By its very nature, a terminated franchisee's continued use of its former franchisor's mark constitutes trademark infringement.[15]

The Franchise Agreement here explicitly stated that the Franchisee only had the right to use the mark solely in connection with the operation of the Franchise and that upon termination, the terminated Franchisee must stop using the Marks.[16] There was evidence submitted that Defendants continued to visit Filta's customers wearing the Franchisor's uniform, pretending to offer services under the Filta brand, all while issuing invoices with payments to be made to KKI.[17]

The court found this sufficient to carry the burden that there was a likelihood of confusion and that Filta is substantially likely to prevail on its trademark infringement-based claims.[18]

2. *Defendants' Continuing Infringement of Filta's Marks will Irreparably Injure Filta*

The court found that, even without the rebuttable presumption of irreparable harm, based on the strong likelihood of customer confusion, Filta met the burden of demonstrating that it will suffer irreparable injury if Defendants' actions were allowed to continue.[19]

3. *The Threatened Injury to Filta Outweighs Any Threatened Harm to Defendants*

The court concluded that Defendants' self-inflicted harm resulting from their choosing to continue to operate in the same industry after terminating the Franchise Agreement was outweighed by the damage done to Filta by the infringement of its marks.[20]

---

[14] *Id.* at *10 (*citing Home Box Off., Inc. v. Showtime/The Movie Channel, Inc.*, 832 F.2d 1311, 1314 (2d Cir. 1987).
[15] *Id.* (*citing Burger King Corp. v. Majeed*, 805 F. Supp. 994, 1002 (S.D. Fla. 1992).
[16] *Id.* at *10-11.
[17] *Id.* at *11-12.
[18] *Id.* at *12.
[19] *Id.* at *13.
[20] *Id.*

4. *The Injunction will not be Adverse to the Public Interest*

The court found that granting the injunction here would actually serve the public interest by preventing the public from being deceived into giving Defendants business under the mistaken belief that they are a legitimate Filta franchisee.[21]

Restrictive Covenants

5. *Filta is Substantially Likely to Succeed on its Claim to Enforce the Restrictive Covenants*

The Franchise Agreement contained post-term restrictive covenants against competition and solicitation which provided that the Franchisee may not for 2 years: 1) compete within the former territory or within 25 miles of the territory; and 2) have contact with any former customers.[22] The court found that Filta was substantially likely to succeed on its claim for breach of the restrictive covenants because the covenants support legitimate business interests. [23]

Florida law evaluates the appropriateness of a restrictive covenant based on its scope and breadth.[24] Under Florida law, a non-competition agreement is enforceable if it seeks to protect "one or more legitimate business interests."[25] The court concluded that Filta had legitimate business interests in 1) protecting its marks and the goodwill associated with them in the relevant territory and industry; 2) preventing the unauthorized use of confidential information obtained through the franchise relationship; and 3) protecting customer goodwill associated with Filta.[26]

The court determined that the restrictions in the covenant were reasonable in time, area, and line of business.[27] This is because the restrictions were tied to the territory assigned to the Franchisees and within a geographic area 25 miles outside of the perimeter of territory formerly assigned to the Franchisees.[28] The two-year duration was also reasonable to allow Filta a fair opportunity to establish a new franchise in the territories.[29]

The court also reinforced Florida's lack of hesitation to enforce non-competition agreements against non-parties to an agreement through which the signing entity/person conducted business.[30] This is in part based on enjoining parties from aiding and abetting

---

[21] *Id.* at *14.
[22] *Id.* at *15.
[23] *Id.* at *16-17.
[24] *Id.* at *16.
[25] *Id.* (*citing* Fla. Stat. § 542.335(1)(b)).
[26] *Id.* at *16.
[27] *Id.* at *17.
[28] *Id.*
[29] *Id.*
[30] *Id.* at *17-18.

a violation of a covenant.[31] The injunction binds the signatory as well as "those identified with them in interest, in privity with them, represented by them or subject to their control."[32] Florida courts are also willing to enforce preliminary injunctions against these parties, notwithstanding that the third party did not sign a non-competition agreement.[33] FRCP 65(d)(2) makes clear that injunction orders bind "parties", and "parties" is defined to include persons who are "in active concert or participation" with the other parties described.[34] The court found that KKI and Farrer were clearly subject to the Franchisees' control and conspired with the Franchisees, and could thus be enjoined.[35]

1. Filta Demonstrates Irreparable Injury

The court concluded a violation of a restrictive covenant creates a presumption of irreparable injury to the person seeking enforcement.[36]

2. The Balance of Harm Weighs in Favor of Filta

The court held that Filta faced substantial harm due to the significant investment of time and resources made in establishing its presence in the territories in connection with this industry which outweighed the self-inflicted harm suffered by Defendants.[37]

3. The Injunction will not be Adverse to the Public Interest

The court found that enforcement of the covenants will serve the public interest as it encourages parties to adhere to contractual obligations and Defendants have not offered any evidence of a public policy interest that outweighs the need to protect Filta's legitimate business interests.[38]

Takeaways

This case reminds franchisors of the importance of crafting restrictive covenants that are tailored appropriately in time, area, and line of business while being narrowly tailored enough to be looked on favorably by the court. More significantly, this case reinforces Florida's commitment to preventing circumvention of post-termination covenants through the use of non-signatories. Despite this protection from the courts, it remains important to continue to take preventative contractual measures to prevent such a scenario. Where appropriate, franchisees' employees should be required to sign confidentiality and/or non-competition agreements to protect proprietary information.

[31] *Id.* at *18.
[32] *Id.* at *19.
[33] *Id.* at *18.
[34] *Id.* at *19.
[35] *Id.* at *20.
[36] *Id.*
[37] *Id.* at *20-21.
[38] *Id.* at *21.

Franchisee covenants should also expansively describe that restrictions apply to agents or other non-signatories that the franchisee may act through.

B. *Laurel Invs., LLC v. Holiday Hosp. Franchising, LLC*, No. 25-cv-10565, 2025 LX 617036, at *2-3 (E.D. Mich. Dec. 30, 2025).

Synopsis

In this choice of law case, the Michigan Eastern District Court held that considerations under Restatement Section 187(2) did not void application of the Georgia choice-of-law provision in the franchise agreement.

Factual Background

Franchisee, Laurel Investments, LLC (Laurel), entered into a License Agreement with franchisor, Holiday Hospitality Franchising, LLC (HHF), permitting Laurel to operate a Holiday Inn-branded hotel in Livonia, Michigan.[39] Laurel, a Michigan limited liability company, was owned by Majid and Lyon Koza, who, along with other related individuals, also served as guarantors of the agreement.[40] HHF, a Delaware entity, is the franchising arm of the Holiday Inn hotel chain.[41] The License Agreement granted Laurel access to its broader "System," including trademarks, reservation platforms, and marketing support.[42]

At the time the agreement was executed, two nearby Holiday Inn Express hotels (offering fewer amenities at lower prices) were already operating in the area, and a third later opened in close proximity.[43] The agreement included several key provisions including: a choice-of-law clause designating Georgia law; language permitting Franchisor to modify certain franchisee benefits during the term; and a clause expressly allowing Franchisor to license additional hotels, including competing brands, in the surrounding area without geographic restriction.[44]

Approximately ten years after entering into the agreement, Laurel and affiliated plaintiffs filed suit in Michigan state court, alleging that the presence and operation of nearby Holiday Inn Express locations created direct and unfair competition, confused consumers, and undermined Laurel's ability to compete effectively as a full-service Holiday Inn property.[45] Plaintiffs further alleged that Franchisor failed to adequately differentiate between the express and traditional brands in its marketing and did not enforce terms of operations at competing locations, amounting to bad faith conduct.[46]

---

[39] *Laurel Invs., LLC v. Holiday Hosp. Franchising, LLC*, No. 25-cv-10565, 2025 LX 617036, at *2-3 (E.D. Mich. Dec. 30, 2025).
[40] *Id.* at *3.
[41] *Id.* at *2.
[42] *Id.* at *3.
[43] *Id.* at *3-4.
[44] *Id.* at *7-16.
[45] *Id.* at *1-5.
[46] *Id.* at *4.

The complaint asserted multiple causes of action including: (1) frustration of purpose; (2) illusory contract; (3) unfair competition under MCL § 445.903; (4) common law unfair competition; (5) breach of the License Agreement; (6) violation of Michigan franchise law; (7) unfair and deceptive practices; and (8) a request for declaratory relief.[47] Franchisor removed the case to federal court and moved to dismiss all claims.[48]

Court's Analysis

Choice of Law

The court first addressed whether the franchise agreement's choice-of-law provision, designating Georgia law, controlled the Laurel Plaintiffs' claims.[49] Applying Michigan's conflict-of-law framework, which follows the Restatement (Second) of Conflict of Laws, the court explained that such provisions are generally enforceable unless either (1) the chosen state lacks a substantial relationship to the parties or transaction, or (2) applying the chosen law would violate a fundamental public policy of a state with a materially greater interest in the dispute.[50]

The court determined that Georgia law governed the majority of the claims. It rejected the argument that Michigan law should apply broadly based on the hotel's location and Michigan's interest in protecting franchisees.[51] Instead, the court found that Georgia had a sufficient connection to the dispute, as the Franchisor was considered a Georgia citizen, thereby satisfying the "substantial relationship" requirement.[52] The court further concluded that applying Georgia law to the non-statutory claims did not contravene any fundamental Michigan public policy, relying in part on precedent reaching similar conclusions in franchise disputes.[53]

However, the court treated the claim brought under the Michigan Franchise Investment Law ("MFIL") differently.[54] Recognizing the MFIL as embodying a fundamental public policy of Michigan, and in light of the parties' agreement on the issue, the court applied Michigan law to that specific statutory claim.[55] Accordingly, the court held that Georgia law governed all claims arising from the franchise agreement except for the MFIL claim, which remained subject to Michigan law.[56] The court then dismissed each of the Laurel Plaintiffs' claims.

---

[47] *Id.* at *5.
[48] *Id.*
[49] *Id.* at *7.
[50] *Id.*
[51] *Id.* at *7-8.
[52] *Id.* at *8.
[53] *Id.*
[54] *Id.*
[55] *Id.* at *8-9.
[56] *Id.* at *9.

Frustration of Purpose

This claim failed as a matter of law since frustration of purpose is an affirmative defense and not a cause of action under Georgia law.[57]

Illusory Contract

Since the License Agreement conferred material benefits upon Laurel and required performance obligations from HHF, the court concluded it was not illusory.[58] The agreement allowing HHF to modify some of Plaintiffs' benefits after-the-fact did not change HHF's obligations and the court's conclusion.[59]

Breach of Franchise Agreement

The court rejected Plaintiffs' claim that HHF breached the License Agreement.[60] No contractual provision prevented HHF from licensing competing locations in close proximity to Plaintiffs.[61] The court also rejected the argument that HHF breached fiduciary duties to Plaintiffs since Georgia does not recognize a fiduciary relationship between franchisors and franchisees.[62]

Declaratory Relief

Since the court dismissed the causes of action upon which declaratory relief was premised this claim was also dismissed.[63]

Unfair Competition Claims

The court found that Plaintiffs failed to meet the requirements to bring this claim as they did not prove they had enforceable trademark rights or that Defendant's unauthorized use of the mark would cause consumer confusion.[64]

Michigan Franchise Law Claims

Plaintiffs claimed that HHF failed to disclose that it "(1) intended to license Holiday Inn Express hotels in close proximity to the Laurel Hotel; (2) marketed the Holiday Inn hotels and Holiday Inn Express hotels in a way that caused consumer confusion; or (3) that it intended not to enforce contractual terms at the Competing Locations."[65] The court concluded that Plaintiffs failed to state a claim under the heightened pleading standards

---

[57] *Id.* at *9-10.
[58] *Id.* at *11.
[59] *Id.* at *13.
[60] *Id.*
[61] *Id.* at *14.
[62] *Id.* at *14-15.
[63] *Id.* at *16.
[64] *Id.* at *16-17.
[65] *Id.* at *18.

for fraud.[66] The court stated that the franchise agreement was clear that HHF had the right to license other hotels without territorial restriction.[67] The court also rejected their argument for lack of specificity in their claims, since Plaintiffs did not plead any examples or indication of how customer confusion occurred or a factual basis for the non-enforcement of terms of operation at other locations.[68]

Request to Replead

Plaintiffs failed to follow proper procedure by failing to file a motion for leave to amend the complaint and instead requested leave to amend in their briefing filed in opposition to Defendant's motion to dismiss.[69]

Takeaways

The Laurel Investments decision highlights several practical lessons for franchisors and franchisees, particularly in the areas of choice of law, contract drafting, and pleading standards. As an initial matter, the case reinforces the importance of carefully analyzing which state's law will govern each claim. While franchise agreements frequently include governing law provisions, courts applying the Restatement (Second) of Conflict of Laws will still scrutinize those provisions. Here, the court largely enforced the Georgia choice-of-law clause, demonstrating that such provisions are likely to be upheld where the franchisor has a substantial connection to the selected state. However, the court's separate treatment of the Michigan Franchise Investment Law underscores that franchise-specific statutes may reflect fundamental state policies capable of overriding contractual provisions. Both franchisors and franchisees should therefore evaluate, on a claim-by-claim basis, whether statutory protections may displace an otherwise applicable choice-of-law clause.

The decision also underscores the critical role of clear contractual language in defining competitive rights within a franchise system. The court relied heavily on the agreement's express provisions allowing the franchisor to license competing locations without territorial restriction, ultimately defeating claims for breach and unfair competition. For franchisors, this illustrates the value of drafting unambiguous provisions preserving system flexibility, particularly with respect to brand segmentation and market saturation. For franchisees, the case serves as a caution to fully understand and negotiate territorial protections, or the absence thereof, at the outset, as courts are unlikely to imply restrictions that are not expressly included in the agreement.

Finally, the case serves as a reminder that franchise litigants must plead claims with specificity and procedural precision. Plaintiffs' failure to adequately allege key elements, such as factual support for consumer confusion, fraud-based claims under franchise statutes, and viable legal theories under the governing law, proved fatal to their

[66] *Id.* at *21.
[67] *Id.* at *19.
[68] *Id.* at *20-21.
[69] *Id.* at *22.

case. Equally important, their failure to properly seek leave to amend further limited their ability to cure deficiencies. In franchise disputes, where claims often intersect with statutory protections and complex contractual frameworks, both franchisors and franchisees should ensure that pleadings are thoroughly developed, factually supported, and procedurally compliant from the outset.

C. *BrightStar Franchising, LLC v. Foreside Mgmt. Co.*, 808 F. Supp. 3d 870 (N.D. Ill. 2025)

Synopsis

In this non-competition case the court analyzed how California's historically strict prohibition on post-termination covenants interacted with a franchise agreement operating under Illinois law.

Factual Background

BrightStar is the franchisor for BrightStar Care Agencies, which has provided in-home care services since 2005.[70] Foreside is a former BrightStar franchisee, run by Mark Woodum; Mark entered four franchise agreements with BrightStar, which he later assigned to Foreside.[71] These agreements included various post-termination obligations, including: 1) restraints on the franchisee's ability to compete against BrightStar in certain geographic regions for 18 months, 2) restraints on the franchisee's ability to solicit BrightStar's customers for 18 months, and 3) obligations to transfer telephone numbers in connection with the franchisee's business.[72] Foreside had executed lateral lease assignments for its two office locations in California (Newport Beach and Mission Viejo) which, upon expiration or termination of the Franchise Agreement, BrightStar would have the right to take possession of.[73]

As the Franchise Agreements neared expiration, Mark Woodsum informed BrightStar's CEO, Andrew Ray, that Foreside did not intend to renew the Franchise Agreements.[74] Foreside then began operating outside of BrightStar's network, and BrightStar sought specific performance of the Collateral lease assignments and to enforce the post-termination obligations present in the Agreements.[75]

BrightStar filed this motion for preliminary injunction to compel possession of the offices under the Collateral Lease Assignments and to enforce the post termination obligations.[76]

---

[70] BrightStar Franchising, LLC v. Foreside Mgmt. Co., 808 F. Supp. 3d 870, 877 (N.D. Ill. 2025).
[71] *Id.* at 877-78.
[72] *Id.*
[73] *Id.* at 878.
[74] *Id.*
[75] *Id.*
[76] *Id.*

Court's Analysis

The party seeking a preliminary injunction must make an initial threshold showing that: (1) it has a likelihood of succeeding on the merits; (2) it will suffer irreparable harm if the injunction is not granted; and (3) traditional legal remedies would be inadequate.

Choice of Law

The court first considered whether the franchise agreement's choice-of-law provision (selecting Illinois) applied to Plaintiff's claims or the law of California where the franchises were located.[77] Illinois follows the Second Restatement of Conflict of Laws, and will generally honor the choice-of-law provisions in a contract unless: "(1) the chosen state has no substantial relationship to the parties or the transaction; or (2) application of the chosen law would be contrary to a fundamental public policy of a state with a materially greater interest in the issue in dispute."[78]

Defendant argued that California law should apply since the franchises were in California and due to the restraints on competition in the Franchise Agreements being unenforceable in California under §16600 of the California Business Code.[79] Plaintiff disagreed, arguing that the California Supreme court case *Ixchel Pharma, LLC v. Biogen, Inc.*,[80] held that §16600 does not per se invalidate such restraints so long as they are made in the context of a commercial relationship, in which a reasonableness test applied.[81] This court agreed with Plaintiff, as the *Ixchel* court specifically referenced franchise agreements as a type that §16600 does not automatically invalidate, and subsequently applied the reasonableness test.[82]

To summarize: (1) *Ixchel* confirms that Section 16600 does not per se invalidate commercial contracts but instead the rule of reason applies, (2) the Franchise Agreements are commercial contracts subject to the rule of reason, and (3) *Ixchel* extends to post-termination covenants such as those found in the Franchise Agreements. The court now returns to the conflict of laws issue.

The court applied Illinois law as the impetus was on Defendant (the party opposing the choice of law provision) to demonstrate a difference in the two states' laws that will make a difference in the outcome, and Defendants did not perform this analysis.[83]

---

[77] *Id.* at 879.
[78] *Id.* (*citing Brown & Brown, Inc. v. Mudron*, 379 Ill. App. 3d 724, 887 N.E.2d 437, 439-40, 320 Ill. Dec. 293 (2008) (paraphrasing the Second Restatement of Conflict of Laws, § 187).
[79] *Id.* at 879-80.
[80] 9 Cal. 5th 1130, 266 Cal. Rptr. 3d 665, 470 P.3d 571 (2020).
[81] *Brightstar*, 808 F. Supp. 3d at 880.
[82] *Id.*
[83] *Id.* at 882.

Breach of Contract

To prevail on a motion for preliminary injunction based on claims for breach of contract under Illinois law, Plaintiff must demonstrate that: (1) a valid and enforceable contract exists, (2) it substantially performed the contract, (3) Defendants breached the contract, and (4) injuries resulted from the breach.[84]

1. Franchise Agreements

a. Valid and Enforceable

The court held that the restrictive covenants in the Franchise Agreements were enforceable under Illinois law because they protected BrightStar's legitimate business interests, including its goodwill, client relationships, and confidential information developed through its franchise system.[85] The court found the restrictions reasonable in scope, limited to the former franchise territory or a 25-mile radius, and in duration, 18 months, and Defendants failed to challenge their reasonableness under Illinois law.[86]

b. Substantial Performance

The court found a strong likelihood this would be met for the Franchise Agreements, since they determined Plaintiff did not substantially breach the Agreements by not complying with pre-dispute obligations, since those obligations do not apply to actions for injunctive relief.[87]

c. Breach

The court found a strong likelihood that Defendants breached numerous post-termination obligations of the Franchise Agreements.[88] It concluded that Defendants likely continued using confidential information and customer data despite contractual prohibitions; violated non-competition provisions by operating a competing business in a restricted area; and held themselves out as a former franchisee despite contrary claims.[89] The court also found likely breaches in failing to return confidential materials, transfer telephone numbers, and cease using BrightStar's proprietary systems and marks, emphasizing that Defendants either did not deny the conduct or offered inadequate explanations (such as claiming the information was "generally known"), which did not excuse noncompliance.[90]

---

[84] *Id.*
[85] *Id.* at 884.
[86] *Id.*
[87] *Id.* at 885.
[88] *Id.* at 885-87.
[89] *Id.*
[90] *Id.*

d. Injury/Irreparable Harm

The court found that BrightStar demonstrated irreparable harm and a lack of an adequate remedy at law sufficient to justify a preliminary injunction.[91] The court emphasized that violations of non-competition and non-solicitation provisions are a classic form of irreparable injury, especially where Defendants continue to operate in the same market and serve former clients.[92] It further reasoned that Defendants' use of confidential information and continued association with BrightStar threaten intangible interests such as goodwill, competitive position, and the integrity of the franchise system that are difficult to quantify, making monetary damages insufficient and injunctive relief appropriate.[93]

e. Balance of Harm/Public Interest

The court held that the balance of harms and public interest favor granting the preliminary injunction.[94] It found Defendants' alleged harms – such as business disruption – were largely self-inflicted and temporary, while BrightStar faced significant, ongoing harm absent relief.[95] The court also emphasized the public interest in enforcing valid contracts and found minimal risk to patient care, concluding that the equities strongly favor BrightStar.[96]

2. Collateral Lease Assignments

The court concluded that the Newport Beach Agreement was likely valid and enforceable, but the Mission Viejo Agreement was not.[97] This was because the underlying Mission Viejo lease was void – Foreside could not contract with itself – so there was no valid lease to assign.[98] However, while Defendants were previously in breach of the Newport Beach Agreement, they had since cured, by surrendering the office.[99] Thus, BrightStar had not sufficiently demonstrated that the lease assignment in the Mission Viejo Agreement was enforceable and Defendants were not in breach of the Newport Beach Agreement, and the court did not find a strong likelihood of success on the merits for the Collateral Lease Assignments.[100]

---

[91] *Id.* at 889.
[92] *Id.* at 888-89.
[93] *Id.*
[94] *Id.* at 890.
[95] *Id.* at 889-90
[96] *Id.*
[97] *Id.* at 882.
[98] *Id.*
[99] *Id.* at 883.
[100] *Id.*

Takeaways

The BrightStar decision underscores the importance of carefully crafting and analyzing choice-of-law provisions and fully pleading all elements of a claim. Franchisors and franchisees should first assess which state's law is likely to govern each claim, particularly how they handle divisive issues such as restrictive covenants or post-termination obligations. Even when a franchise agreement contains a governing law clause, many courts will examine whether the selected law has a substantial relationship to the parties and the transaction and whether applying that law would conflict with a fundamental public policy of another state with a stronger interest. However, as seen in BrightStar, it is important to remember that not only must you plead that there exists a difference in the laws of the two states that warrants departing from the choice of law provision, you must also show that the different law would result in a different outcome. Here, after the court rejected Defendants' argument that the restraints on competition were per se unenforceable under California law, they never presented an actual analysis showing that California's rule of reason differs from Illinois' reasonableness standard, resulting in the court applying Illinois law.

The ruling also clarifies how courts may evaluate restrictive covenants in franchise agreements when California law is implicated. By relying on *Ixchel Pharma, LLC v. Biogen, Inc.*, the court indicated that non-competition provisions in commercial, business-to-business relationships such as franchising may be evaluated under a rule-of-reason analysis rather than automatically invalidated under California's prohibition on restraints of trade. This distinction reinforces that franchise relationships are commercial arrangements rather than employment relationships and supports franchisors' ability to protect legitimate business interests such as goodwill, proprietary systems, and brand integrity through reasonable covenants. The decision underscores the importance of precise choice-of-law provisions, clear drafting that defines the commercial nature of the relationship, and well-supported allegations demonstrating the reasonableness of restrictive covenants in scope and duration.

D. Non-*compete* Judicial Legal Update – Virginia

Franchise lawyers should take notice of a legislative legal update currently happening in Virginia. As of April 13, 2026, Governor Abigail Spanberger signed into law Virginia HB 69/SB240. [101] This legislation makes it unlawful to enter into a franchise agreement that restricts the right of a franchisee to engage in the business of offering, selling, or distributing goods or services after termination or expiration of the agreement; or where the restriction of the franchisee's right to do business is part of the settlement to a controversy, except where such settlement is approved by a court.[102] Beginning on

[101] *HB69 Retail franchise agreements; governing law, competition restrictions,* LEGISLATIVE INFORMATION SYSTEM, https://lis.virginia.gov/bill-details/20261/HB69 (last visited April 14, 2026); *SB240 Retail franchise agreements; governing law, competition restrictions,* LEGISLATIVE INFORMATION SYSTEM, https://lis.virginia.gov/bill-details/20261/SB240 (last visited April 14, 2026).
[102] *Id.*

July 1, 2026, Virginia will ban the offer or sale of a franchise containing a post-term non-compete provision in the franchise agreement. These restrictions now make Virginia the most restrictive state in the country on franchise post-term non-competition provisions.

III. Arbitration Cases

A. *Northeast Emergency Apparatus LLC v. Mine Respirator Co. LLC*, No. 2:25-cv-00556-SDN, 2025 LX 565810 (D. Me. Dec. 23, 2025).

Synopsis

The following is an arbitration case that discusses how the drafting of the arbitration provision in a franchise agreement affects the question of who determines arbitrability and analyzes several challenges to the enforcement of an arbitration provision.

Factual Background

Plaintiff, Northeast Emergency Apparatus LLC ("NEA"), a distributor of personal protective equipment and safety devices, sued its manufacturer MSA Safety Sales LLC ("MSA Safety"), to enjoin them from terminating their agreement.[103] The parties' relationship was governed by a distribution agreement under which NEA sold MSA Safety products.[104] The Agreement contained several provisions relevant to the dispute, including:

- **Arbitration Clause**: Any controversy, claim, or dispute "arising under" the agreement must be resolved through arbitration in Pittsburgh, Pennsylvania under rules of the American Arbitration Association (AAA);
- **Choice-of-Law Provision**: The agreement is governed by Pennsylvania law.
- **Termination Provision**: Either party could terminate the agreement upon thirty days' written notice.[105]

NEA alleged that the termination violated the Maine Franchise Laws for Power Equipment, Machinery and Appliances, 10 M.R.S. §§ 1361–1370 (the "Franchise Laws"), and the Maine Unfair Trade Practices Act ("MUTPA").[106] NEA also sought injunctive relief to prevent termination of the distributorship.[107] While the litigation **proceeded,** MSA

[103] *Ne. Emergency Apparatus LLC v. Mine Respirator Co. LLC*, No. 2:25-cv-00556-SDN, 2025 LX 565810, at *2-3 (D. Me. Dec. 23, 2025).
[104] *Id.*
[105] *Id.* at *2.
[106] *Id.*
[107] *Id.* at *3.

Safety moved to compel arbitration under the Agreement and the Federal Arbitration Act ("FAA").[108]

On December 4, 2025, the court granted NEA's motion for a temporary restraining order, enjoining termination of the agreement.[109] NEA subsequently filed a motion for leave to file a second amended complaint, seeking to add a claim under the Maine Farm Machinery, Forestry Equipment, Construction Equipment and Industrial Equipment Dealerships Act, 10 M.R.S. §§ 1285–1298.[110] NEA argued that the Act cast doubt on the validity of the Agreement's arbitration provision because it requires arbitration to occur in the dealer's principal place of business in Maine.[111] The court here addressed the motion to amend the complaint and the motion to compel arbitration.[112]

Court's Analysis

Motion for Leave to Amend

Acknowledging FRCP 15(a)(2)'s liberal policy to allow amendments in the absence of undue delay, bad faith, futility, or the absence of due diligence, the court granted the motion to amend.[113] Marking the absence of the above factors, the court noted that NEA filed the motion shortly after the case was removed to federal court and before any responsive pleading had been filed.[114]

Motion to Compel Arbitration

Under the FAA, a court can compel arbitration where the moving party shows: (1) "a valid agreement to arbitrate exists"; (2) they are "entitled to invoke the arbitration clause"; (3) "the other party is bound by that clause"; and (4) "the claim asserted comes within the clause's scope."[115]

1. Choice of Law

The court looked to state contract law to determine the validity of the arbitration provision.[116] Applying Maine's conflict of law rules, the court determined that Pennsylvania law applies to determine validity of arbitration.[117] Under Maine law, a court must enforce a choice-of-law provision except where the chosen state lacks a substantial relationship to the parties or applying its law would violate a fundamental public policy of

---

[108] *Id.*
[109] *Id.*
[110] *Id.*
[111] *Id.*
[112] *Id.*
[113] *Id.* at *4-5.
[114] *Id.*
[115] *Id.* at *5.
[116] *Id.* at *7.
[117] *Id.* at 7-9.

Maine.[118] The court concluded a substantial relationship existed because MSA Safety is incorporated and headquartered in Pennsylvania and neither party claimed applying Pennsylvania law would be contrary to Maine public policy.[119]

2. Delegation

The court next concluded that the question of arbitrability was for the court to decide and not the arbitrator.[120] The court rejected MSA's contention that, by incorporating the AAA rules, the parties had delegated the question of arbitrability to the arbitrators.[121] To overcome the presumption that arbitrability is decided by the courts, the agreement must contain clear and unmistakable evidence of an intent to do so.[122] While the incorporation of arbitration rules can sometimes demonstrate an intent to delegate arbitrability, the agreement did not identify a specific set of AAA rules or contain explicit language assigning those threshold issues to the arbitrator.[123]

3. A Valid Agreement to Arbitrate Exists

NEA contested whether an agreement to arbitrate the merits of the dispute existed, arguing that its claims under the Franchise Law and Act are not subject to arbitration because the statutes rendered either 1) the entire agreement, or 2) the arbitration provision void as against public policy.[124] The court indicated that NEA could only avoid arbitration by succeeding on an argument that invalidates the arbitration provision itself.[125] Regarding NEA's argument under the Franchise Laws, the court determined that that the challenge was under the purview of the arbitrator since NEA challenged the validity of the entire agreement rather than directing the challenge specifically to the arbitration provision.[126]

NEA next argued that under the Franchise Act the arbitration provision was void because it required arbitration in a venue outside of the city where NEA has a principal place of business.[127] However, the court determined that, under Pennsylvania law, even if the Act prohibited the agreement from providing for arbitration in such a venue, that would only void that provision mandating that location, and not the entire arbitration provision.[128]

---

[118] *Id.* at *8.
[119] *Id.*
[120] *Id.* at *14.
[121] *Id.* at *9.
[122] *Id.* at *10.
[123] *Id.* at *11-13.
[124] *Id.* at *15.
[125] *Id.* at *17.
[126] *Id.* at *16-17.
[127] *Id.* at *15.
[128] *Id.* at *17-18.

4. NEA's Claims Fall Within the Scope of the Arbitration Provision

The court also found that, unless expressly provided for otherwise, it is the court and not the arbitrator that decides the scope of the arbitration clause.[129] As long as at least some issues are covered by the agreement to arbitrate others are presumed arbitrable as well.[130] Here, the clause was expansive, stating that "[a]ny controversy, claim or dispute arising under this Agreement shall be finally settled by arbitration."[131] Applying Pennsylvania law and the federal policy favoring arbitration, the court concluded that this language was sufficiently broad to encompass disputes relating to the termination of the distributorship agreement.[132]

Authority to Compel Arbitration

Finally, the court concluded that although arbitration is required, it does not have the authority to compel arbitration.[133] The FAA directs courts to enforce arbitration agreements within the judicial district in which they sit.[134] Therefore, since the agreement specified Pittsburgh, Pennsylvania as venue for arbitration the court transferred the case to United States District Court for the Western District of Pennsylvania to effectuate the arbitration agreement.[135]

Takeaways

This decision underscores the importance of carefully drafting arbitration provisions in franchise and distribution agreements. Parties should clearly specify the governing arbitration rules and expressly state whether questions of arbitrability are delegated to the arbitrator, as courts will not infer delegation absent "clear and unmistakable" evidence. When the court is deciding the issue of arbitrability, parties seeking to avoid arbitration should be careful to focus their challenges on the enforcement of the arbitration provision itself. Attacks on the contract as a whole and on more discrete issues such as venue most likely will be unsuccessful at preventing arbitration. Franchisors and franchisees should consider how state franchise or dealer protection statutes may affect venue or enforceability of arbitration provisions. Even where such statutes impose restrictions, courts may sever only the offending portion of a clause rather than invalidate arbitration entirely, reinforcing the importance of precise drafting and awareness of potentially applicable state laws when structuring dispute resolution provisions.

---

[129] *Id.* at *18.
[130] *Id.* at *19.
[131] *Id.*
[132] *Id.* at *19-20.
[133] *Id.* at *21-22.
[134] *Id.* at *22.
[135] *Id.*

B. *Marcus Corp. v. MKD Inv. Holdings, LLC*, No. 25-CV-1131-SCD, 2026 LX 36633, at *2 (E.D. Wis. Jan. 26, 2026).

Synopsis

In this arbitration case, the court held that the question of arbitrability for whether a non-signatory to a franchise agreement agreed to arbitrate is to be decided by the court absent clear and unmistakable evidence of consent.

Factual Background

Defendant MKD Investment Holdings, LLC (MKD) entered into several franchise agreements with Verlo Mattress to open Verlo mattress franchises in Texas.[136] The franchise agreements contained arbitration provisions that incorporated the American Arbitration Association rules.[137] In December of 2024, MKD filed a demand for arbitration against Verlo Mattress, Stallman, Marcus Corporation, and Marcus Investments for violations of Wisconsin and Texas statutes, negligent misrepresentation, and fraudulent inducement.[138] Dirk Stallman was the former president of Verlo Mattress, who signed the agreements in his capacity as officer.[139] It is not clear how Marcus Corp. or Marcus Investments are involved, other than being entities alleged to be related to Verlo.[140] Stallman and the two Marcus entities were not signatories to the franchise agreements, and objected to the arbitration.[141]

The arbitrator concluded the entities were properly joined to the arbitration.[142] The Marcus entities and Stallman subsequently filed a Declaratory Judgment Action seeking a declaration they were not subject to the arbitration provisions and had no obligation to arbitrate with MKD.[143]

Court's Analysis

Jurisdiction

The court relied on Seventh Circuit factors to determine whether a district court should exercise jurisdiction over a declaratory judgment.[144] These factors asked, for example, whether the litigation would settle the controversy regarding the parties' legal relationship, whether other, better, remedies were available, and whether their

---

[136] *Marcus Corp. v. MKD Inv. Holdings, LLC*, No. 25-CV-1131-SCD, 2026 LX 36633, at *2 (E.D. Wis. Jan. 26, 2026).
[137] *Id.* at *1-2.
[138] *Id.* at *3.
[139] *Id.* at *2.
[140] *Id.* at *1.
[141] *Id.*
[142] *Id.*
[143] *Id.* at *2.
[144] *Id.* at *5-6.

relationship is subject to arbitration.[145] The court concluded that adjudication was appropriate; it would clarify the relationships at issue, there was no evidence it was done for the purpose of "procedural fencing," and there was no conflict between federal and state authority of the issue.[146] The court also concluded that arbitration cannot be compelled absent an actual agreement to arbitrate.[147]

The Question of Arbitrability

The court highlighted that arbitration is a matter of contract, and the court held that whether a non-signatory agreed to arbitrate is a question of arbitrability for judicial determination and not a question to be decided by the arbitrator absent clear and unmistakable evidence of consent.[148] Here, Plaintiffs allege that they were never a part of an agreement to arbitrate in the first place.[149] Since the existence of the agreement to arbitrate itself is in dispute, the court held that it is the court that must answer this question.[150] The court rejected MKD's argument that questions on arbitration were delegated to AAA by way of the AAA rules themselves that the arbitration agreement called for.[151] However, the court found that, here, the ultimate issue is whether Plaintiffs agreed to arbitrate with MKD and concluded that that issue cannot be logically answered by the arbitrators.[152]

Waiver of Judicial Review

MKD argued that plaintiffs waived their right to judicial review by failing to raise these arguments with the arbitrator, as they did not participate in the arbitration when they had already previously objected to it.[153] The court disagreed. The court looked to other case law that found that participating in an arbitration proceeding by objecting to arbitrability does not make the arbitrator's decision binding.[154] Thus, Plaintiffs did not lose judicial review by objecting. The motion to dismiss was denied, allowing the declaratory judgment action to proceed.[155]

Takeaways

This decision emphasizes the nature of arbitration as being a pathway created only by contract that does not exist without an agreement to enter it. Courts are unwilling to disregard corporate structures and separate legal existences and assume that affiliates,

---

[145] *Id.*
[146] *Id.* at *6-7.
[147] *Id.* at *7.
[148] *Id.*
[149] *Id.* at *6-7.
[150] *Id.* at *8-9.
[151] *Id.* at *9.
[152] *Id.* at *10.
[153] *Id.*
[154] *Id.* at *10-12.
[155] *Id.* at *12-13.

officers, or other related entities agreed to an arbitration provision without clear proof supporting that claim.

In the franchise context, this decision emphasizes the importance of clear and detailed drafting in our definitions of the parties involved and in our arbitration provisions themselves. If a franchisor intends an arbitration provision to encompass and be binding on other entities or individuals beyond the direct franchisee signing, this should be clearly and directly addressed in the agreement. Additionally, if you desire the arbitrator to resolve all issues, even the issues of interpretation and application of the arbitration provision, this should be clearly and explicitly outlined in the agreement. In the end, this decision highlights the importance of having clear and explicit contractual language.

Parties on the other side of the dispute should recognize the permissibility of courts to allow them to contest the arbitrability of an issue without waiving their right to a review of the matter by the courts. In conclusion, this decision did not answer whether non-signatories ultimately can be compelled to arbitrate. However, it does answer the question that it is the court that has the authority to make that decision when a party's consent is challenged.

IV. Contract Disputes

A. *Isla Verde Serv. Station, Inc. v. Puerto Rico Energy, LLC*, 2025 WL 3539149 (D.P.R. Dec. 10, 2025).

Synopsis

This case involves a court's issuance of a preliminary injunction enjoining a franchisor's ability to terminate a franchise agreement following the court's analysis of the issues under the specific standards required by the *Petroleum Marketing Practices Act*.

Factual Background

Plaintiff was a family-owned gas location in Carolina, Puerto Rico.[156] Plaintiff and Defendant had been parties to a franchise agreement for 12 years, before it expired and they continued on a month-to- month basis.[157] Under the Agreement, Defendant provided gasoline and owned the premises of the service station; Plaintiff was responsible for rent, purchasing gasoline, and operating the station.[158] Before the expiration of the original agreement, Defendant informed Plaintiff that it intended to move to a "dealer-owned" "dealer-operated" model.[159] To continue operating the franchise this would have required

[156] *Isla Verde Serv. Station, Inc. v. P.R. Energy, LLC*, No. 25-01655 (MAJ), 2025 LX 514610, at *1 (D.P.R. Dec. 10, 2025).
[157] *Id.* at *1-2.
[158] *Id.* at *2.
[159] *Id.*

Plaintiff to purchase the premises while continuing to purchase gasoline from Defendant.[160]

The parties negotiated the sale of the franchise, its equipment and inventories to Defendant, however Plaintiff alleged there were multiple defects in the bargaining process, such as 1) Defendant did not obtain any independent appraisal of the value of the service station during the course of negotiations; 2) Plaintiff alleged that "no bona fide, station-specific third-party offer existed for the Isla Verde Service Station; and 3) Plaintiff alleges that, before presenting its offer, Defendant had already "initiated discussions with real estate brokers and the third party" offeror.[161]

Court's Analysis

Under FRCP 65, a court may issue a temporary restraining order if: (A) specific facts in an affidavit or a verified complaint clearly show that immediate and irreparable injury, loss, or damage will result to the movant before the adverse party can be heard in opposition; and (B) the movant's attorney certifies in writing any efforts made to give notice and the reasons why it should not be required.[162]

Here Plaintiff moved for an emergency order under the Petroleum Marketing Practices Act (PMPA).[163] This statute provides that the court shall grant emergency injunctive relief if 1) the franchisee plaintiff shows that "there exist sufficiently serious questions going to the merits to make such questions a fair ground for litigation[,]" and (2) "the court determines that, on balance, the hardships imposed upon the franchisor by the issuance of such preliminary injunctive relief will be less than the hardship which would be imposed upon such franchisee if such preliminary injunctive relief were not granted."[164]

a. *Plaintiff has raised "sufficiently serious questions going to the merits" that constitute "fair ground[s] for litigation."*

The PMPA establishes minimum federal standards governing the termination and nonrenewal of franchise relationships for the sale of motor fuel by franchisors or suppliers of such fuel due to the vast disparity in bargaining power between franchisee and franchisor in the market.[165] To this end, the PMPA provides for a general prohibition against termination or nonrenewal of franchises.[166] However, the PMPA provides that termination or nonrenewal is permissible where it is based on specific statutory grounds enumerated in 15 U.S.C. § 2802(b).[167] Even where appropriate grounds exist, under applicable circumstances, the Act requires a franchisor to (1) make "a bona fide offer to

---

[160] *Id.*
[161] *Id.* at *3-4.
[162] *Id.* at *4-5.
[163] *Id.* at *5.
[164] *Id.* at *6.
[165] *Id.*
[166] *Id.* at *7.
[167] *Id.*

sell, transfer or assign" its interest in the premises to the franchisee, and (2) offer the franchisee a right of first refusal of at least 45 days duration before exercising its non-renewal rights.[168]

Plaintiff identified two defects in the bargaining process that they argued constituted fair grounds for litigation. First, they argued that Defendant lacked statutory authority to exercise any enumerated non-renewal right.[169] Defendants claimed in its notice to Plaintiff that the grounds for nonrenewal were based on a failure of the franchisor and franchisor to agree to changes in the provisions of the franchise, if such changes were 1) made in good faith and in the normal course of business; and 2) the failure was not the result of franchisor's insistence on changes for the purpose of preventing renewal.[170]

Plaintiff argued that Defendant's decision to move to a "dealer-owned, dealer-operated" business model, an its subsequent offers to sell the premises to Plaintiff (1) were not made in good faith, (2) were not made in the ordinary course of business, and (3) were made in order to prevent renewal of the franchise.[171]

The court agreed that Plaintiff at the very least raised serious questions regarding these elements. Plaintiff had alleged that Defendant 1) did not obtain any independent appraisal of the value of the service station during the course of negotiations and that the asking price for the property was substantially inflated; 2) that Defendant's offers were calculated to trigger a rejection; and 3) that Defendant actually intended to use the property as part of a "credit-offset arrangement" with a third-party.[172] The court therefore concluded that Plaintiff had raised fair ground for litigation under this theory.[173]

Second, even if Defendants had legitimate grounds for nonrenewal, Plaintiffs insist that Defendants nevertheless violated the Act by failing to make "a bona fide offer to sell, transfer or assign" its interest in the premises to Plaintiff.[174] This is an objective test, based on the offeror's general practice for selling property and the purchase price must be near the fair market value.[175] The court concluded that Plaintiffs sufficiently questioned this issue with their allegation that 1) Defendant did not obtain any independent appraisal of the value of the service station during the course of negotiations, and made an offer to Plaintiff that over-valued the property by approximately 70%; and 2) Defendant had already initiated discussions with real estate brokers and the third party offeror before presenting Plaintiff with its offer.[176]

---

[168] *Id.* at *7-8.
[169] *Id.* at *8.
[170] *Id.*
[171] *Id.* at *9.
[172] *Id.* at *9-10.
[173] *Id.* at *10.
[174] *Id.*
[175] *Id.*
[176] *Id.* at *10-11.

b. On balance, the issuance of injunctive relief will impose lesser hardships on Defendant than Plaintiff would face in the absence of injunctive relief.

The court concluded that, on balance, the potential hardships that Defendant faces if emergency injunctive relief was granted were outweighed by the potential hardships that Plaintiff would face in the absence of relief.[177]

Takeaways

It is important to note that the holding of this case should be analyzed in the context of the facts, procedural posture, and applicable statute. This decision came early in the litigation so it is still to be determined whether the statute was violated or the Franchisor acted in bad faith. What it does tell us is that special issues and questions are raised for franchisors in the petroleum field that are looking to move on or navigate from their relationship with their franchisees. Franchisors must be aware of the lower pleading standards and heightened requirements presented by the PMPA. It is vital that franchisors seeking to change franchisees under this statute maintain detailed documentation of their business rationale, consistently apply standards across their franchisees, and obtain legitimate valuations in support of their propositions. This is reinforced by the court's hesitance to recognize non-traditional "offers" (here a proposed credit-offset arrangement) in place of a bona-fide offer from a third party in the ordinary course of business. The bona-fide offer requirement is fact-intensive and judicial scrutiny of offers is heightened where procedural irregularities exist.

B. *Big Tree Invests., LLC v. Urbanize, LLC*, No. 27-CV-25-7049, *2 (Minn. Dist. Ct. Feb. 2, 2026).

Synopsis

In this case the Minnesota District court analyzed the extent of protections provided by a waiver and release provision in a mutual termination agreement between a franchisor and franchisee.

Factual Background

John Golle was a co-founder and CEO of the franchisor Urbanize Farms, LLC, who entered into a franchise agreement with Big Tree Investments, LLC as franchisee on April 26, 2022.[178] On November 14, 2022, franchisee and franchisor entered into a Mutual Termination Agreement (MTA) for the Franchise Agreement; the MTA contained an extensive release provision which released Urbanize Farms and all of its officers, directors, employees, representatives, and other affiliates from all claims arising out of the franchise agreement.[179]

---

[177] *Id.* at *12.
[178] B*ig Tree Invests., LLC v. Urbanize, LLC*, No. 27-CV-25-7049, *2 (Minn. Dist. Ct. Feb. 2, 2026).
[179] *Id.* at *3.

Franchisee brought claims for violation of the Minnesota Franchise act, fraud, negligent misrepresentation, and breach of contract against the franchisor and three co-founders; all other claims were resolved and only the claims against Golle remained.[180]

Court's Analysis

Franchisee sued Golle individually as a "control person" for the franchisor.[181] However, the court ruled that even with all facts in the complaint accepted as true, plaintiff could not maintain their claims because Golle, as co-founder, fell squarely within the category of person who was released from liability under the MTA.[182] The court found that the release language in the MTA was extensive, clear and unambiguous and should be enforced.[183]

Franchisee argued that the claims should survive because factual issues existed regarding the enforceability of the release and included allegations that the release was fraudulently produced.[184] The court rejected these arguments, in large part because the complaint itself did not assert any allegations of fraud, misrepresentation or mistake relating to the formation of the MTA.[185] No allegations existed about any act, omission, or misconduct that occurred for the inducement to enter into the MTA.[186]

Finally, the court recognized that Plaintiffs have also already settled and released their ability to void the MTA, thus they cannot now add a claim to void the MTA.[187] Accordingly, the plain language of the MTA did not allow Plaintiffs to pursue the claims against Golle since the Complaint included no facts, allegations, or claims that would void the MTA.[188]

Takeaways

This case emphasizes the importance of clearly outlining the parties involved, in both the agreement itself and in any waiver provisions, when separating from a franchise relationship. Clearly presenting the parties released from claims and the types of claims being released in broad, clear, and unambiguous language provides the greatest opportunity for a waiver provision to be looked upon favorably by the court.

Additionally, this case reminds us of the critical role that proper planning of the litigation strategy plays. First, the court looked very unfavorably upon Plaintiffs attempt to raise an argument for fraud with respect to the MTA since they had not included any

---

[180] *Id.* at *4.
[181] *Id.* at *7.
[182] *Id.* at *5.
[183] *Id.* at *7.
[184] *Id.* at *8.
[185] *Id.* at *9.
[186] *Id.*
[187] *Id.*
[188] *Id.* at *10.

allegation in their complaint regarding such a claim. Secondly, Plaintiffs failed to recognize that by settling and releasing claims with the Franchisor, they had settled with the only party that they had entered into the MTA agreement with. Thus, the court found that not only did their pleadings and claims show they were not seeking to void the MTA, but they had also released the only party they had the ability to raise the claim against. This result emphasizes the need to broadly plead any potential claims you may be able to raise and to be aware of the arguments you may be cutting off when entering settlements.

V. AI Cases

A. *United States v. Heppner*, No. 25-cr-00503-JSR (S.D.N.Y. Feb. 6, 2026)

Synopsis

In this case, the court determined that documents created by a client using generative AI tools were not protected by privilege.

Factual Background

This case answered a novel issue: whether when a user communicates with a publicly available AI platform in connection with a pending criminal investigation, are the AI user's communications protected by attorney-client privilege or work product doctrine? The court answered no.[189]

Defendant, Heppner, believed he would be indicted for federal securities and wire fraud.[190] Without being prompted by his attorney, he personally conducted research related to the claims using "Claude" a private AI platform.[191] Heppner prepared reports that outlined defense strategy and what he might argue with respect to the facts and the law that they anticipated the government might charge.[192] The government seized these communications which outlined Defendant's facts, defense strategy, and arguments.[193] Heppner's counsel asserted attorney-client privilege and the work product doctrine arguing: 1) Heppner had input information that he had learned from counsel; 2) Heppner had created the documents for purpose of speaking with counsel to obtain legal advice; and 3) Heppner had subsequently shared the contents of the AI documents with counsel.[194]

[189] *United States v. Heppner*, No. 25-cr-00503-JSR (S.D.N.Y. Feb. 6, 2026).
[190] *Id.* at 3.
[191] *Id.*
[192] *Id.*
[193] *Id.*
[194] *Id.* at 3-4.

Court's Analysis

Attorney-Client Privilege

The documents were not protected by attorney-client privilege because they were not confidential communications with an attorney for the purpose of obtaining legal advice.[195] The court concluded it was not a communication with an attorney because Claude is not an attorney and all recognized privileges require a human relationship.[196] The court also reasoned they were not confidential because Heppner communicated with a third party AI platform which also contains in its privacy policy language that Claude's owner collects both user inputs and Claude's outputs.[197] The policy reserved the right to disclose this data to third parties.[198]

Finally, Heppner did not communicate with Claude at the direction of his attorney.[199] The court recognized this prong's analysis may be different if his attorney had directed him to consult AI, thereby making Claude more akin to a lawyer's agent.[200]

Work Product Doctrine

The AI documents did not merit protection under the work product doctrine because, even assuming that they were prepared in anticipation of litigation, they were nevertheless not prepared by or at behest of counsel, nor did they reflect defense counsel's strategy.[201] Since the documents were prepared at Heppner's own volition, although the documents did affect counsel's strategy going forward, they did not reflect counsel's strategy at the time Heppner created them.[202]

This reasoning follows the second circuit's intended purpose for the doctrine, which is to protect lawyers' mental processes.[203]

Takeaways

Heppner demonstrates the importance of having appropriate policies regarding the use of AI. It is critical counsel communicates openly with clients regarding the clients' use of AI and make sure they understand how you incorporate AI into your practice. When AI is used it should be supported with sufficient documentation to reflect it was used at the direction of counsel and in anticipation of litigation. Potentially this case raises the

---

[195] *Id.* at 5.
[196] *Id.* at 5-6.
[197] *Id.* at 6.
[198] *Id.*
[199] *Id.* at 7.
[200] *Id.*
[201] *Id.* at 9.
[202] *Id.*
[203] *Id.* at 11.

question of whether Franchise Agreements should encode standards and rules governing what franchise information is restricted from being uploaded or introduced to AI programs.

Whether a franchisor or franchisee, it is critical that all employees, agents, partners, and other people working with you in your network understand your company's protocol and guidance governing the use of AI and that rules are set in place that limit potential exposure of confidential information. Interactions with generative open-AI platforms should be treated as potentially discoverable.

B. *Lifetime Well LLC v. IBSpot.com Inc.*, No. 25-5135, E.D. Pa., 2026 U.S. Dist. LEXIS 13363

Synopsis

In this AI hallucination case, the court sanctioned two Pennsylvania- and New York-based attorneys after the court identified multiple AI hallucinations in their briefs and issued both monetary and non-monetary sanctions.

Factual Background

The sanctioned conduct in this case arose out of a copyright infringement claim filed by e-commerce retailer Lifetime Well LLC (Lifetime) against IBSpot.com (IBSpot) for violating copyright and trademark law by selling Lifetime's hearing aid on their website.[204] After the case progressed and Lifetime obtained default judgment, IBSpot obtained local counsel who moved for the admission pro hac vice of a New York Attorney.[205] IBSpot filed a motion to dismiss the case, said motion being signed by both the primary New York Counsel and local Pennsylvania counsel, with local counsel filing the motion.[206]

The court identified eight instances where the authorities offered by the attorneys either did not stand for the propositions asserted, arose from inapposite jurisdictions, or had inaccurate quotations.[207] When responding to the show cause, the primary New York attorney offered various excuses as to the lapse in accuracy, noting an extremely short timeline of several days to file the motion upon notice of the case from their client and that those days were also holidays requiring parental responsibilities.[208] Finally, the attorney swore that she assigned a new law clerk to assist in preparing the motion, asked the law clerk to double check all citations, and it was not until after the court's show cause order that she was alerted of the issue and realized, unbeknownst to the firm, that the

[204] *Lifetime Well LLC v. IBSpot.com Inc.*, No. 25-5135, 2026 LX 13236, at *4 (E.D. Pa. Jan. 26, 2026)
[205] *Id.*
[206] *Id.* at *5.
[207] *Id.* at *5-6.
[208] *Id.* at *7.

clerk used AI to prepare the filing.[209] The local counsel also conceded to not being aware of the use of AI or the hallucinated case law.[210]

Primary counsel responded by firing the law clerk and implementing a zero-tolerance immediate termination AI policy.[211] Local counsel responded by voluntarily completing a CLE course on the ethical and responsible use of AI and by entering an agreement with primary counsel on the case that all future filings must be submitted 48 hours in advance with a table of authorities to which the attorney will facilitate a thorough review.[212]

Court's Analysis

The court concluded that both attorneys had violated FRCP 11 by flagrantly ignored their obligations in regards to the filing and analyzed how to impose sanctions.[213] The court also looked unfavorably upon primary counsel firing a new lawyer rather than train them when the ultimate responsibility was on the senior counsel.[214] As to local counsel, while the court found he did not meet the standard that local counsel is held to, ensuring the integrity of filings, they found his response was appropriate.[215]

Both Attorneys Violated Rule 11

The court relied on precedent from the Supreme Court of PA to conclude that in order to satisfy the affirmative duty of Rule 11 an attorney must inquire into both the facts and the law before filing papers with the court.[216] "Obligations imposed under subdivision (b) obviously require that a pleading, written motion, or other paper be read before it is filed or submitted to the court."[217] As to AI specifically, the Court recognized the Rule 11 does not prohibit the use of AI, however it does require that the parties verify that they are not submitting briefs with fictitious law or other information.[218] The signing attorney is the final auditor for all legal and factual claims, regardless of who assisted in the research or drafting.[219] This is a nondelegable responsibility, by signing the attorney represents not only the fact that the paper is factually and legally accurate but also the fact that they personally have applied their judgment to it.[220]

---

[209] *Id.*
[210] *Id.* at *9.
[211] *Id.* at *8.
[212] *Id.* at *9.
[213] *Id.* at *21.
[214] *Id.* at *10.
[215] *Id.*
[216] *Id.* at *11.
[217] *Id.*
[218] *Id.* at *13.
[219] *Id.*
[220] *Id.* at *17-18.

The court was unconvinced by primary counsel's argument that AI was used unbeknownst to her or the firm, as that did not change any of her responsibilities outlined above as a signing attorney.[221] Additionally, the court believed that opposing counsel identifying a false citation gave primary counsel notice and opportunity to review the rest of the filing and correct it, which they did not do until the court's show cause order.[222] Local counsel did not dispute that his conduct violated Rule 11, accepted responsibility, and recognized the court's legitimate concerns.[223] Due to both attorneys' actions taken to remedy their mistakes the court declined to refer them to the disciplinary board.[224]

Monetary and Non-Monetary Sanctions on Primary Counsel

The court found primary counsel's conduct extended beyond what a purely non-monetary sanction would adequately address to achieve Rule 11's goal of deterrence.[225] The court looked unfavorably upon her firing of the law clerk, lack of immediate self-correction (especially as compared to Local Counsel's actions), failure to correct the briefing upon notice of an error by opposing counsel, and her shifting explanations.[226]

The court imposed a $4,000 sanction as a means to reinforce accountability and deter repetition of the conduct.[227] The court also required her to submit a copy of the cover letter to the proceedings with attachments to all counsel and presiding judges of the other two matters the new attorney had used AI in.[228]

Non-Monetary Sanctions on Local Counsel

The court was most concerned with local counsel's near-blind acceptance of papers drafted by an attorney not admitted to the Bar of this court and willingness to file those papers under his name without citing legal authority.[229] However, the court looked favorably upon his acceptance of responsibility, completion of continuing education, and corrective steps adopting new policy as local counsel.[230]

The court required local counsel to submit the order, memorandum and his AI policy to the Philadelphia Intellectual Property Lawyers Association and request they be shared with its membership during its next meeting to serve as a lesson on the risks of AI and the duties of local counsel.[231]

---

[221] *Id.* at *18-19.
[222] *Id.* at *19.
[223] *Id.* at *21.
[224] *Id.* at *24.
[225] *Id.* at *22.
[226] *Id.* at *22-23.
[227] *Id.* at *23-24.
[228] *Id.* at *24.
[229] *Id.* at *26.
[230] *Id.* at *26-27.
[231] *Id.* at *27.

Takeaways

This decision again highlights the importance of being cognizant of the use of AI by all parties involved in a matter. Additionally, this decision is of particular significance in the franchise industry, where disputes frequently involve trademark enforcement and infringement, system standards disputes, and other claims that typically involve multi-jurisdictional litigation. While AI may offer efficiency in dealing with high-volume issues it creates a material risk if it is not paired with sufficient verification processes. Franchisors in particular should be attentive to their own AI policies, oversight structures, and AI policies of the local counsel they work with, ensuring that local counsel meaningfully reviews filings. Failure to do so can not only create the risk of sanctions but opens potential weakened pleadings and potentially failed enforcement of their claims.

C. AI Sanctions: *When* Attorneys Don't Comply

In comparison to *Lifetime*, the case *Whiting v. City of Athens*[232] provides an example of how a court responds where the attorneys at issue submit work with AI hallucinations and fake citations and then refuse to comply with show cause orders and instead seek to procedurally attack said order.[233] Unlike in *Lifetime*, where the attorneys complied with the show cause order and then attempted to provide explanations and justifications for the AI hallucinations they submitted, here the attorneys did not respond to the directives of the show cause order and instead challenged the order.[234] The attorneys argued that the show cause order was "void on its face for failing to include a signature of an Article III judge," was "motivated by harassment of the Respondent attorneys," and reflected illegal ex-parte communications within the court.[235]

The court found that sanctions beyond those normally prescribed under FRAP 38 were required based on the attorneys behavior, and also brought sanctions under its inherent authority.[236] Not only was the attorney's appeal to the court meritless, the court concluded that they attempted to use the court system to force a result not obtainable under applicable law by relying on known fabricated authority and then when presented with an opportunity to explain themselves failed to do so and instead challenged the order asking for the explanation.[237]

This level of behavior resulted in harsh sanctions from the court, requiring: 1) the attorneys to reimburse appellees in full for their attorneys' fees on appeal in all three appeals; 2) the attorneys to pay double costs to appellees for costs incurred under 28 U.S.C. § 1920 on appeal in all three appeals; 3) the attorneys to each pay $15,000 to the

[232] Nos. 24-5918/5919, 25-5424, 2026 LX 132948 (6th Cir. Mar. 13, 2026).
[233] *Id.* at *1-2.
[234] *Id.* at *2-3.
[235] *Id.* at *3.
[236] *Id.* at *10-13.
[237] *Id.* at *12.

court as punitive sanctions; and 4) the clerk to file a copy of this order with the chief judge to consider disciplinary proceedings.[238]

What *Whiting* and *Lifetime* clearly illustrate is how to properly respond to the court when issues of AI hallucinations occur in submissions to the court. Always seek to provide explanations where appropriate and to illustrate sincere mistakes, however do not seek to avoid responsibility. Comply with orders from the court and take accountability where mistakes were made. Attempts to avoid this responsibility and challenge a tribunal seeking explanations may result in extreme sanctions.

VI. Summation

A non-all-inclusive variety of selective recent cases and trends to peak the interest of franchise lawyers, while keeping in mind that there most likely have been related case holdings issued that may fortify the holdings or changed the holdings and the take aways to consider. Stating the obvious, always the obligation the lawyers to check the cites and status of the cases and statutes involved to remain current.

[238] *Id.* at 18-19.

International Franchise Association
58th Annual Legal Symposium
May 18–19, 2026

Staying Ahead of Cybersecurity Risks: Protecting Your Franchise Business from Attackers and Litigants Alike

Jennifer Daskal
Venable, LLP
Washington, DC

The estimated global cost of cybercrime is projected to rise by over $6.4 trillion between now and 2029, reaching a staggering $15.6 trillion over the next four years.[239] Technological developments, including the proliferation of increasingly sophisticated artificial intelligence, decrease the cost of entry for cybercriminals, making it easier to breach systems, steal credentials, and wreak havoc on companies, big and small alike.

Strong cybersecurity is no longer optional. It is essential to protect every business, both franchisors and franchisees. It is required by key regulators and insurers. And it serves several critical functions, including mitigating the costs of an attack, legal risk, and reputation harm.

The following discusses cybersecurity trends and developments, the relevant regulatory framework in the United States, and the key steps that every business should take to mitigate the risk of cyber-attack, ensure compliance with regulatory obligations, protect against legal liability, and manage potential reputational harm.

I. Evolving Cybersecurity Risks

Over the past decade, cyber threats have increased dramatically in both frequency and scale. Malicious actors are exploiting the growing number of vulnerabilities in systems and networks to intentionally cause harm, disrupt operations, steal sensitive data, and undermine trust. This strategic environment is driven by a complex mix of compounding factors, including escalating geopolitical tensions, growing dependence on opaque and interconnected supply chains, and the rapid adoption of emerging technologies—all of which create new entry points and expand the attack surface for cyber adversaries. [240]

Nation-state actors and their proxies are increasingly sophisticated at exploiting vulnerabilities in the digital ecosystem. Financially motivated criminals are also a growing threat, with ransomware actors increasing in scope and sophistication—aided in significant part by the ability to target identified victims. Ransomware attackers are also adopting more aggressive tactics, including extortion schemes that combine threats to leak stolen information and doxxing (a form of digital abuse that exposes sensitive personal information). The annual global costs of ransomware continue to rise and are predicted to reach $275 billion by 2031, with attackers expected to strike every two seconds. [241]

---

[239] Peter A. Jensen, *Estimated cost of cybercrime worldwide 2018–2029 (in trillion U.S. dollars)*, Biocomm AI (July 30, 2024), https://blog.biocomm.ai/2024/09/07/cnbc-estimated-cost-of-cybercrime-worldwide-2018-2029-in-trillion-u-s-dollars/.

[240] *See, e.g.,* World Econ. Forum, *Global Cybersecurity Outlook 2025* 4 (Jan. 13, 2025), https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

[241] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/. Costs are defined to include negotiations and payouts, damage and destruction of data, stolen money, downtime, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration

Other types of cyber-enabled crime also pose business risks. The FBI's Internet Crime Complaint Center reports year-over-year increases in advertising scams, business email compromise fraud, and identity theft, driven in part by the availability of behavioral data that enables highly targeted deception.[242]

Increasingly sophisticated AI, including agentic and generative AI, creates new challenges. AI has accelerated phishing and automated system reconnaissance, elevated the capabilities of less sophisticated threat actors, and amplified those of advanced threat actors. The cybersecurity company CrowdStrike reports an 89% increase in attacks by AI-enabled adversaries between 2024 and 2025.[243] Sophisticated adversaries also target the AI integrated into businesses, seeking to inject malicious prompts that launch attacks by generating unauthorized commands.

II. Regulatory Environment & Liability Risks

There is no overarching federal cybersecurity (or privacy) law in the United States. Instead, a broad patchwork of often overlapping federal sector-specific laws and regulations, as well as state law, sets the standards companies are required to meet. The following details key regulations, regulators, and requirements that apply. That said, and as is obvious, every fact pattern is different, and companies should consult with counsel to identify and implement appropriate compliance regimes.

A. General Liability

Section 5 of the Federal Trade Commission (FTC) Act. The Federal Trade Commission serves as the baseline cybersecurity enforcement agency for most businesses that operate in the United States. Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices," and in several cases, the FTC has concluded that poor cybersecurity can violate this prohibition.[244] The FTC has, for example, brought enforcement actions against those who have "unreasonable" data security practices, and against those who promise a certain level of security but fail to deliver on those promises. Notably, most FTC cybersecurity-related cases occur *after* a breach; the FTC is unlikely to investigate entities in the absence of a triggering event that brings a specific entity to the FTC's attention. Most cases end with a consent decree under which the FTC requires

---

and deletion of hacked data and systems, reputational harm, legal costs, and potentially, regulatory fines.

[242] Fed. Bureau of Investigation, *Internet Crime Report 2024* 13–15 (Apr. 23, 2025), https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

[243] https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike-2026-Global-Threat-Report.pdf (p 15)

[244] See 15 U.S.C. § 45(a). FTC jurisdiction includes most businesses "affecting commerce" in the United States. Certain, specified industries are exempted from FTC jurisdiction, including banks, savings and loan institutions, common carriers, and air carriers—all of which are regulated by separate entities. *Id.*

a company to put in place a comprehensive security program, replete with reporting and compliance provisions. [245]

Through various publications and enforcement actions, the FTC has set out a series of standards for what companies need to do to ensure "reasonable" security, including: (i) data minimization measures that protect against the unnecessary collection of personal data and store personal data for only as long as needed; (ii) access controls for sensitive data; (iii) strong, secure passwords, multifactor authentication, and other good credential measures, such as no sharing of passwords; (iv) properly configured encryption and other tools to store and transmit data securely; (v) mitigation of well-known vulnerabilities; (vi) adoption of an incident response plan and other information security plans; (vii) monitoring and validation of network access; (viii) implementation of effective endpoint security; (ix) requirements that service providers, such as cloud-service providers and others that maintain company data, also employ strong security; (x) regular testing and updating of systems; and (xi) training of employees and personnel.[246]

Franchisors that centralize data, fail to enforce franchisee compliance with basic security measures, and make brand-level security representations that overstate their actual cybersecurity practices can be held liable for the actions of their franchisees. Federal courts have confirmed affirmed that "unreasonable" security practices—including storing credit card data in plain text, allowing the use of easily-guessed passwords, and failure to limit access to and monitor its systems—can be subject to FTC regulatory action.[247] That said, FTC cases against franchisors are infrequent, given that the FTC generally targets the "control point," meaning the entity that controls the data, designs, the systems, and makes consumer-facing representations. Franchisors that centralize and remain control over the franchise systems technology and data are more likely to be a target of FTC action than those who do not.

---

[245] For a helpful analysis of recent FTC cybersecurity cases, *see* Isabella Wright & Maia Hamin, "'Reasonable' cybersecurity in forty-seven cases: The Federal Trade Commission's enforcement actions against unfair and deceptive cyber Practices," *The Atlantic Council* (June 12, 2024), https://www.atlanticcouncil.org/in-depth-research-reports/report/reasonable-cybersecurity-in-forty-seven-cases-the-federal-trade-commissions-enforcement-actions-against-unfair-and-deceptive-cyber-practices/#:~:text=Over%20most%20of%20the%20last,that%20instigated%20the%20FTC's%20complaint

[246] *See, e.g.,* FTC, *Start with Security: A Guide for Businesses* (August 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/920a_start_with_security_en_aug2023_508_final_0.pdf; see also Wright & Hamin, *supra* note 7 (identifying the "de facto list" of unreasonable security practices from 47 FTC cybersecurity cases between 2002 and 2024).

[247] See, e.g., *FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015); *In re Marriott Int'l, Inc. Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447 (D. Md. 2020).

***State Actions and Civil Liability*.** Entities that evade FTC liability can still be subject to state regulatory action and civil liability, as described below.

State Unfair or Deceptive Acts or Practices Laws. All states have laws prohibiting unfair or deceptive acts or practices ("UDAP laws") that mimic and are enforced similarly to Section 5 of the FTC Act. These laws are generally enforced by state attorneys general, with some state laws also providing for consumer litigation. In several cases, state attorneys general have taken the position that failure to adopt reasonable security measures constitutes an "unfair" practice, including in cases against franchisors. Several of these have also been supplemented by class actions.[248]

State Breach Notification Law. All 50 states have data breach notification laws in place. These require notification when there is unauthorized access to or acquisition of sensitive personal information, such as a name plus Social Security number or other personally identifying information. The kinds of information that trigger notification requirements, the timing of notification, and the scope of the required notification vary by state. Some breaches, for example, require notification only to affected individuals, while others also require notification to state attorneys general or credit bureaus.

State Affirmative Security Requirements. A minority of state laws impose generally applicable data security requirements. For example, the New York SHIELD Act requires businesses that own or license New York residents' private information to "develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity" of the information, including the implementation of a data security program that complies with a specified list of administrative, technical, and physical safeguards.[249] New York also imposes strict cybersecurity requirements for any New York-regulated financial institutions, including maintenance of a cybersecurity program, certain cybersecurity governance structures, a vulnerability management program, due diligence over third-party service providers, and certain specific measures, such as use of encryption, multi-factor authentication, and establishment of an incident response plan.[250] Massachusetts requires any entity that owns or licenses personal information about a Massachusetts resident to maintain "comprehensive information security plans" and to employ specified computer system security requirements, including the use of encryption, secure user authentication protocols, access control measures, and employee education and training.[251] Kansas law requires a holder of personal information to implement and maintain "reasonable" practices to protect personal information.[252] An Alabama law also requires covered entities to maintain reasonable security measures to protect "sensitive personally identifying information" (i.e., information that would trigger the state's data

---

[248] *See, e.g.*, *In re Wawa, Inc. Data Sec. Litig.*, No. 2:19-cv-06019, 2021 WL 1818494 (E.D. Pa. May 6, 2021) (addressing claims arising from malware-based payment card breach across retail locations); *In re Hyatt Hotels Corp. Data Sec. Breach Litig.,* No. 1:16-cv-04750 (N.D. Ill.); Mass. Off. of the Attorney Gen., *Rhode Island Company to Pay $230,000 in Penalties Over Data Breach Impacting More Than 3,000 Massachusetts Residents* (July 21, 2022).

[249] N.Y. Gen. Bus. § 899-bb

[250] N.Y. Comp. Codes R. & Regs. Tit. 23 § 500.0 *et seq.*

[251] 201 Mass. Code Regs. §§ 17.03-17.04.

[252] Kan. Stat. Ann. § 50-6,139b.

breach notification law) against a security breach.[253] The Alabama law identifies specific practices to consider when implementing "reasonable" security measures.[254] In addition, some state laws impose security requirements for government contractors.[255]

State Omnibus Privacy Laws. Several states also have omnibus consumer privacy laws that require "controllers" to maintain reasonable security measures to protect personal data. State attorneys general usually enforce these laws, although some states have their own privacy regulators, and some also authorize private rights of action. Such laws generally require controllers to establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect personal data.[256] The laws also include data minimization requirements that prohibit controllers from processing personal data unnecessarily.

B. Sector Specific Requirements

Gramm-Leach-Bliley Act (GLBA). GLBA applies to franchisors and franchisees that *offer financing or credit*. Depending on the circumstances, it can also apply to those that operate centralized payment or loyalty systems to collect financial data across franchisees.[257] The implementing requires a written security program (the so-called "Safeguards Rule"), that includes the following: (i) a risk assessment; (ii) identification of an individual responsible for the security program; (iii) implementation of core safeguards (to include encryption, multi-factor authentication, access controls, and secure development practices); (iv) assessment and monitoring of vendors; (v) penetration testing and other monitoring; (vi) implementation of an incident response plan; and (vii) regular reporting to senior leadership and/or the company Board. As of May 2024, the Rule also requires regulated entities to notify the FTC as soon as possible, and no later than 30 days after discovery, of a security breach involving the information of at least 500 customers.[258]

Health Insurance Portability and Accountability Act (HIPAA). HIPAA applies to *health providers, plans, and clearinghouses*, as well as "business associates" that manage health data. The law and applicable regulations set standards for when personal health information can be used or disclosed, mandate cybersecurity safeguards for electronic protected health information, and require reporting and notification in the event of a breach.[259]

---

[253] Ala. Code § 8-38-3.

[254] Id. § 8-38-3(b).

[255] For example, a Pennsylvania law requires an entity that maintains personal information on behalf of the Commonwealth to develop a policy governing "reasonably proper storage" of the information. Pa. tit. 73, 2305b(a).

[256] *See., e.g.,* N.J. Stat. Ann. § 56:8-166.12(a)(3); Tenn. Code Ann. § 47-18-3204(a)(3); Tex. Bus. & Com. Code Ann. § 541.101(a)(2); Va. Code Ann. § 59.1-578(a)(3).

[257] *See* 15 U.S.C. § 6801 *et seq.*

[258] *See* 16 C.F.R. part 314.

[259] 45 C.F.R. part 164, subpart C; 45 C.F.R. §§ 164.306, 164.308, 164.310, 164.312 (2025).

Securities and Exchange Commission (SEC) Cybersecurity Rule. This rule covers *publicly traded companies* and requires an annual disclosure in which companies must describe their processes for managing, assessing, and identifying cybersecurity risks, including how they are monitored, and their Board's role in overseeing such risks.[260] The Rule also requires disclosure of a "material" cyber incident within four days of determining materiality. An incident is determined "material" if a reasonable investor would consider it important—a standard that accounts for factors such as potential financial loss, operational disruption, reputational harm, and legal exposure. The reporting requirement is triggered at the time of determination, not at the time of discovery.[261]

Banking Reporting Requirements. Covered *banking organizations* are required to notify their relevant banking regulator—either the Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, or Federal Reserve—within 36 hours of discovering a computer-security incident that has materially disrupted or degraded, or is likely disrupt or degrade the ability or viability of operations, customer access to accounts, or the stability of the financial sector. Bank service providers are required to notify at least one bank point-of-contact of any computer-security incident that has materially disrupted or degraded, or is likely to disrupt or degrade covered services for more than four hours. [262] The rules for credit unions are slightly different—requiring federally insured credit unions to provide notice to the National Credit Union Association no later than 72 (versus 36) hours after occurrence of a "reportable cyber incident," which is defined by the regulations to include a disruption of business operations, vital member services, or a member operation system, among other appliable criteria.[263]

Family Educational Rights and Privacy Act (FERPA). Franchisors and franchisees that operate *education systems or institutions* and receive federal funding are covered by FERPA, as are *ed-tech franchisors and test-prep franchises* that contract with public schools and receive student data. FERPA and its implementing regulations prohibit the disclosure of students' personally identifiable information without consent or an applicable exception and require the use of "reasonable methods" to protect against unauthorized disclosures.[264]

Children's Online Privacy Protection Act (COPPA). COPPA and its implementing rule apply if a franchisor or franchisee collects data of children under 13. Entities are required to establish and maintain "reasonable procedures" to protect the

---

[260] 17 C.F.R. §229.106; Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Securities Act Release No. 33-11216, Exchange Act Release No. 34-97989, 88 Fed. Reg. 51896 (Aug. 4, 2023)

[261] 17 C.F.R. § 249.308 (Form 8-K, Item 1.05); *TSC Indus., Inc. v. Northway, Inc.*, 426 U.S. 438, 449 (1976) (defining information to be "material" if there is a substantial likelihood that a reasonable investor would consider it important).

[262] *See Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers*, 86 Fed. Reg. 6643 (effective April 1, 2022).

[263] 12 C.F.R. § 748.1

[264] 34 C.F.R. § 99.31.

confidentiality, security, and integrity of personal information collected from children. This is defined to include annual assessments for identifying risks to confidentiality, security, and integrity of such data; implementation of safeguards to address those risks; regular testing and monitoring of the safeguards; and oversight of other operators, service providers, and third parties that have access to such data to ensure the use of "reasonable" data protection measures. [265]

C. Contractual Requirements and Insurance Policies

Payment Card Industry Data Security Standard (PCI DSS). While neither a law nor a regulation, PCI DSS effectively operates as such. It applies to any franchisor or franchisee that *handles credit card payments* and is enforced through contractual requirements with major credit card brands. Non-compliance can result in significant fines and is often cited as evidence of unreasonable security practices in civil litigation, state enforcement actions, and FTC enforcement actions. The standards mandate implementation of 12 core requirements designed to ensure network security, protect data (via encryption and secure transmission), protect against malware, identify and authenticate users, and ensure entities monitor and test networks and maintain a strong information security policy, including a documented incident response plan. [266]

Other Contractual Obligations*.* Clients and business partners of franchisors and franchisees are also likely to require the implementation of reasonable cybersecurity practices and to provide notice in the event of a breach. The details vary in terms of what is required, what triggers notification obligation, and how quickly notification is required. Entities should review these provisions before accepting them, incorporate reporting obligations into incident response plans, and work with counsel to determine the scope and wording of notifications.

Cyber Insurance*.* Cyber insurance policies typically require insured entities to maintain reasonable and appropriate security measures. This is typically a condition of coverage. It can also be a basis for denial of claims if the security measures in place do not match the representations made to the insurer. Insurers also increasingly look for, and in many cases require, the implementation of specific controls, such as multi-factor authentication, endpoint detection, patch monitoring, effective backup and recovery controls, "least privilege" access controls (meaning access is limited to those with a business need for access), and security awareness training for employees. Insurance policies also require notification after a breach—generally either "immediately" or "as soon as practicable." Many policies also require notification regarding suspected breaches, even if not yet confirmed.

---

[265] 16 C.F.R. § 312.8

[266] *See* Payment Card Industry Security Standards Council, *Payment Card Industry Data Security Standard (PCI DSS) v.4.0.1* (2024).

D. Data Transfers/Security Rules

Franchisors and franchisees that are engaged in international transfers of data also need to comply with both non-U.S. cybersecurity rules (the details of which are outside the scope of this article) and certain security restrictions applicable to the transfer of certain U.S. data to certain foreign countries and entities.

Specifically, franchisors and franchisees are bound by the restrictions included in the Final Rule on Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons (the "Bulk Data Rule")[267] and the Protecting Americans' Data from Foreign Adversaries Act[268] which prohibit the transfers of specified categories of data to certain foreign countries and entities. These are categorical prohibitions, based on security concerns.

The Bulk Data Rule also imposes a set of security requirements on vendor, employment, and investment agreements that involve the transfer of bulk U.S. sensitive data and government-related data to either a country of concern (currently China, Cuba, Iran, North Korea, Russia, and Venezuela) or a covered person. Covered persons include residents of a country of concern; entities that are organized, chartered, or have a principal place of business in a country of concern; employees or contractors of such persons or entities; and any entity that is 50% or more owned, individually or in the aggregate, by a country of concern or other covered person.

Absent an applicable exemption, such transfers *must* comply with specified security requirements promulgated by the Cybersecurity and Infrastructure Security Agency, as well as other applicable due diligence, auditing, and reporting obligations. These requirements include operational and system-level requirements, data-level requirements, and implementation of a data compliance program.[269]

E. Class Actions: Data Breaches

All businesses, including franchisors and franchisees, are at risk of becoming defendants in class actions and other plaintiff litigation in the wake of a data breach. While the Supreme Court has made clear that speculative risk of future data misuse in the wake

---

[267] 28 C.F.R. part 202 (2025);

[268] Protecting Americans' Data from Foreign Adversaries Act of 2024, Pub. L. No. 118-50, div. I, 138 Stat. ___ (2024) (codified at 15 U.S.C. § 9901 et seq. (2024))

[269] See Cybersecurity and Infrastructure Security Agency, *Security Requirements for Restricted Transactions* (January 2025), https://www.cisa.gov/sites/default/files/2025-01/Security_Requirements_for_Restricted_Transaction-EO_14117_Implementation508.pdf; *see also* Jennifer Daskal, Kelly DeMarchis Bastide & Caitlin Clarke, *A Closer Look at the Data Security Requirements in DOJ's Bulk Data Rule* (June 3, 2025), https://www.venable.com/insights/publications/2025/06/a-closer-look-at-the-data-security-requirements

of a breach is not enough to establish standing,[270] some lower courts have concluded that: (i) a *material* risk of future misuse could establish standing, if sufficiently imminent and substantial; and (ii) time loss and other costs associated with monitoring for misuse are concrete harms.

In *Webb v. Injured Workers Pharmacy*, [271] for example, the First Circuit found standing based on the fact that the data was exposed in a targeted attack rather than inadvertently. The data was particularly sensitive, as it included a name and a linked Social Security number, and *other* data taken in the attack had already been misused. The court found "concrete, present harm" based on the lost time and effort spent monitoring accounts to protect against identity theft—even though there was no evidence that the data had been published, let alone misused.

Conversely, in Holmes v. Elephant Insurance,272 the Fourth Circuit found that only some of the putative plaintiffs had standing: those whose driver's numbers were listed on the dark web. By contrast, breach victims whose driver's licenses had been compromised but not yet disclosed on the dark web or otherwise misused lacked standing. The fact that the hackers posted *others'* driver's licenses was not, in the Fourth Circuit's view, sufficient to establish an imminent threat to those whose data had not yet been made publicly available.

In sum, breach cases require concrete harm, which is clearly established if there is demonstrated misuse of data, such as fraudulent charges or identity theft. But future harm can establish standing if it is concrete and imminent. Publication of sensitive data on the dark web can be sufficient to establish standing, depending on the circumstances. And, per *Webb,* publication may not even be necessary to establish standing if other factors establish sufficient risks and there are concrete harms in terms of credit monitoring.

III. Proactive Steps Every Company Can Take

When it comes to cybersecurity, prevention is the best medicine. As reflected in case law, standards bodies, and regulatory frameworks, there are baseline cybersecurity practices that *every* company should implement. This applies to both franchisors and franchisees, no matter how big or small. Core elements include secure passwords and access controls, encryption, endpoint and malware detection, and auditing and penetration testing to ensure effectiveness; adoption and implementation of strong governance frameworks, including information-handling, data-retention, and cyber-incident-response plans; and employee training.

[270] See *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021).
[271] 72 F.4th 365 (1st Cir. 2023).
[272] 156 F.4th 413 (4th Cir. 2025).

Best Practice: Standards Bodies and Certification Frameworks

Several standard bodies and certification programs establish best practices to guide entities in implementing effective cybersecurity programs. Compliance will not fully protect against breaches, but it will provide a strong defense in the wake of regulatory action or litigation due to a breach. Conversely, failure to comply with core standards is often used as evidence of "unreasonable" cybersecurity practices.

Key standards frameworks include:

- The *National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0,* which provides guidance for all organizations, regardless of size or sector, to better manage and reduce cybersecurity risk. NIST is not a certification body but sets out a risk management framework that companies can use to create a strong cybersecurity posture consistent with business needs.[273]

- The *Information security, cybersecurity, and privacy protection – Information security management systems – Requirements (ISO/IEC 27001)* lays out internationally recognized sets of standards for managing information security management systems, coupled with a certification program by third-party auditors. Certifications last for three years, although annual assessments are also required. The certification audit can be costly, with the cost depending on the size and complexity of the business. [274]

- *CIS Security Controls* are a recommended set of 18 cyber defense actions designed to thwart some of the most pervasive attacks; these recommendations have been endorsed by NIST and others.[275]

- As discussed above, compliance with the *Payment Card Industry Data Security Standard (PCI DSS)* is required for any entity that processes credit cards.

- Other frameworks set standards for specific industries. *Systems and Organizational Controls (SOC02),* for example, is an auditing framework focused on ensuring that service providers, such as cloud service and "software as a service" providers. [276] Contractors within the US Department of Defense supply

[273] U.S. Dep't of Commerce, National Institute of Standards and Technology, *The NISCT Cybersecurity Framework (CSF) 2.0* (Feb. 26, 2024), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.
[274] International Organization for Standardization & International Electrotechnical Commission *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements.* https://www.iso.org/standard/27001
[275] Center for Internet Security, *CIS Critical Security Controls Version 8.1* (June 2024), https://www.cisecurity.org/controls
[276] American Institute of Certified Public Accountants. *Audit and Assurance: SOC 2*. AICPA & CIMA, https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2.

chain that handle non-public data are obliged to comply with the requirements of the *Cybersecurity Maturity Model Certification.*[277]

Testing and Training

Even the best laid plans of mice and men can go awry. It is therefore essential to test and train systems and governance structures.

This includes at least annual penetration testing of systems, exercising incident response plans, regular employee training on key policies (such as information-handling requirements and data-retention rules), and basic cyber hygiene (including using strong, secure passwords and being aware of phishing risks).

Exercises are a particularly effective way to identify gaps, work through operational coordination issues, ensure the leadership team (including CEOs, Chief Information Officers, and the General Counsel) has clarity about roles and responsibilities in the event of a breach, and highlight leadership prioritization of strong cybersecurity practices and policies.

Breach Responses

As with any emergency situation, the first step is to stop the bleeding. What is required will, of course, depend on the facts. Even fact-gathering can be complicated, as it can often be hard to know the scope of an incident as it evolves. Exacerbating the challenge, communication itself may be compromised based on the nature of the breach.

Among the many things that need to be considered in the wake of an incident:

- Assessing the Situation / Bringing in a Forensics Team
- Whether and when to engage law enforcement
- Potential reporting obligations
- Contractual requirements with clients
- Communications, both externally and internally
- Reputational and litigation risk

Entities that have exercised their incident response plans are likely to be more adept, agile, and effective in response. Entities that take proactive responses to harden their networks and put in place effective governance structures will also be much better positioned, vis-à-vis regulators, litigators, and the court of public opinion.

---

[277] *See* 32 C.F.R. part 170 (establishing the Cybersecurity Maturity Model Program); DFARS 252.204-7021 (contractor requirements); U.S. Dep't of War, Chief Information Officer, *About CMMC,* https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2

IV. Specific Issues Relevant to Franchise Systems

Franchise systems present a unique set of cybersecurity challenges because they operate as networks of semi-independent businesses that are nonetheless connected through shared branding, and often shared systems and data. This hybrid structure creates vulnerabilities that neither fully centralized corporations nor completely independent small businesses typically face.

Inconsistency in cybersecurity practices across franchisees creates risks for the brand as a whole. While a franchisor may establish standards or provide recommended tools, individual franchisees often differ in their financial resources, technical expertise, and prioritization of cybersecurity. Depending on the degree of centralized technical controls, franchisees may also independently select local information technology providers or software solutions that are not vetted by the franchisor; such vendors likely differ in how much they prioritize cybersecurity. An uneven security posture creates weak points that attackers can exploit.

Franchisees that rely on shared platforms, including point-of-sale systems, customer relationship management tools, and internal communication networks, are particularly vulnerable to these risks. A breach at a single franchise location can provide attackers with access to broader systems, enabling lateral movement across the network. In this way, a localized vulnerability can quickly escalate into a system-wide incident.

Data protection and regulatory compliance also pose challenges. Both franchisors and franchisees may handle sensitive customer information, including payment data and personally identifiable information. Even if it is clear in internal documents that a specific franchisee is responsible for safeguarding consumer information, regulators, courts, and customers may not see it that way. Consumers tend to associate any breach with the overarching brand, meaning that reputational damage extends far beyond the affected franchise location.

Ultimately, franchise cybersecurity is shaped by a fundamental tension between control and autonomy. Effective cybersecurity management requires each player in the system to implement strong cybersecurity practices at both the technical and governance levels. This, in turn, requires clear policies, standardized security requirements, and strong collaboration across the franchise. Without such alignment, the entire franchise system remains vulnerable to its weakest link.

V. Conclusion

With rapid developments in AI, the cyber threat environment is becoming increasingly more sophisticated and complex. Meanwhile, entities are governed by an increasingly complex set of overlapping rules, standards, insurance requirements, and contractual obligations relating to cybersecurity. The good news is that there are core steps that every entity can—and should—take to protect against threat actors, regulators, and litigants alike. Good cybersecurity cannot be an afterthought but needs to be treated as an essential element of every franchise system's business model.

International Franchise Association
58th Annual Legal Symposium
May 18-19, 2026

Using AI in the Employment Process: Recent Developments You Need to Know

Bradford J. Kelley
Littler Mendelson, P.C.
Washington, DC

I. Introduction

Artificial intelligence ("AI") is rapidly reshaping the modern workplace, transforming how organizations recruit, manage, and evaluate workers across the entire employment lifecycle.[278] Employers increasingly rely on AI-driven tools for resume screening, applicant engagement and scheduling, automated video interviews, productivity and safety monitoring, meeting transcription, and advanced analytics designed to assess employee performance and predict future success. When thoughtfully designed and responsibly deployed, these technologies can deliver substantial benefits, including improved efficiency, enhanced workplace safety, reduced bias and subjectivity, stronger compliance mechanisms, and expanded economic opportunity for both employers and workers. AI has the potential not only to streamline operations, but also to enable faster, more informed, and more consistent decision-making at scale.[279]

At the same time, the rapid adoption of AI in employment introduces significant and increasingly scrutinized risks. Improperly designed or poorly governed systems can exacerbate discrimination, enable invasive surveillance, undermine wage-and-hour compliance, and contribute to workforce displacement.[280] Emerging technologies such as generative AI and deepfakes add an additional layer of concern, enabling the creation of synthetic images, audio, or video that may be weaponized as tools of harassment or intimidation in the workplace.[281] These developments raise complex legal and operational challenges, particularly where AI systems operate with limited transparency or insufficient human oversight.

Compounding these risks is a rapidly evolving and fragmented regulatory environment. Federal, state, and local regulators have moved aggressively to address AI's role in employment decisions, often through overlapping and sometimes inconsistent frameworks. Measures such as New York City's AI law governing automated employment decision-making tools illustrate the growing appetite for AI-specific regulation, even as questions persist about clarity, enforceability, and practical effectiveness.[282] Employers operating across multiple jurisdictions, especially franchise systems, must navigate a

---

* Bradford J. Kelley is a Shareholder in Littler Mendelson, P.C.'s Washington, DC office. He previously served as Chief Counsel to a Commissioner of the U.S. Equal Employment Opportunity Commission ("EEOC"), and as a Senior Policy Advisor in the U.S. Department of Labor's Wage and Hour Division. He is also a former U.S. Army infantry and intelligence officer and a combat veteran of the Iraq War.

[278] *See* Bradford J. Kelley & Andrew B. Rogers, *The Sound and Fury of Regulating AI in the Workplace*, HARVARD J. ON LEGIS. (2025), https://journals.law.harvard.edu/jol/2025/12/06/the-sound-and-fury-of-regulating-ai-in-the-workplace/.

[279] *Id.*

[280] *Id.*

[281] *See* Bradford Kelley & Alyesha Asghar, *AI-Driven Harassment Poses New Risks for Employers*, LAW360 (Jan. 20, 2026), https://www.law360.com/articles/2431002/ai-driven-harassment-poses-new-risks-for-employers.

[282] *See* Kelley & Rogers, *supra* note 1.

complex compliance landscape while continuing to deploy AI technologies that are increasingly central to competitiveness and scalability.

Against this backdrop, this Article proceeds in three parts. Part II examines how AI is currently being used throughout the employment process, with particular emphasis on its role within franchise systems and other scalable business models. Part III provides an overview of the main legal risks associated with AI in the workplace. Part IV analyzes the emerging regulatory frameworks governing workplace AI, focusing on key developments at the state and local level. Part V surveys recent litigation shaping the contours of liability for AI-driven employment practices, including claims targeting employment discrimination, privacy, transparency, and vendor liability. Together, these developments underscore a central theme of this Article: while AI introduces new tools and unprecedented scale, it operates largely within existing, technology-neutral employment law frameworks, placing a premium on governance, oversight, and strategic deployment rather than reactive compliance. In light of the increasingly complex regulatory environment and expanding litigation exposure, Part VI articulates a framework of recommended practices intended to guide employers toward proactive risk management, robust governance, and the responsible, legally compliant deployment of AI across the employment lifecycle.

II. The Growing Use of AI in the Workplace

A. AI in the Workplace: An Overview

AI has rapidly evolved from a novel technological tool into a foundational component of modern workplaces, fundamentally reshaping how work is performed, decisions are made, and value is generated across industries.[283] By 2025 and into 2026, adoption has accelerated at a remarkable pace, with recent data indicating that approximately 26% of employees now use AI tools at least several times per week.[284] This widespread integration reflects not only technological advancement, but also a structural shift in how organizations operate. AI-powered technologies, including generative AI systems and increasingly sophisticated agentic tools, are now embedded across core business functions. These systems automate routine and repetitive processes, synthesize vast quantities of data into actionable insights, and increasingly operate as collaborative partners alongside human employees. As a result, workers are able to redirect their efforts toward higher-value activities such as strategic planning, creative problem-solving, and interpersonal engagement. At the organizational level, employers are leveraging AI to drive operational efficiencies, reduce costs, and unlock new revenue opportunities.[285]

---

[283] *See generally* Keith E. Sonderling, Bradford J. Kelley, & Lance Casimir, *The Promise and the Peril: Artificial Intelligence and Employment Discrimination*, 77 U. MIAMI L. REV. 1 (2022).

[284] Gallup, *Frequent Use of AI in the Workplace Continued to Rise in Q4*, Gallup Workplace Insights (Jan. 14, 2026), https://www.gallup.com/workplace/701195/frequent-workplace-continued-rise.aspx.

[285] *See* Sonderling, Kelley & Casimir, *supra* note 6.

Within the employment lifecycle, employers, particularly in scalable business models such as franchising, are deploying AI-driven tools at virtually every stage, including recruitment, candidate screening, hiring, workforce management, and retention. These technologies encompass resume-parsing algorithms, automated video interview platforms, personality and behavioral assessments, and predictive analytics designed to forecast employee performance, engagement, and attrition. As staffing challenges intensify, AI-enabled franchise support systems will increasingly equip leaders to proactively identify workforce risks, standardize coaching and performance management practices, and streamline operational workflows across large, geographically dispersed networks.[286]

AI is also transforming core workplace functions. In customer-facing roles, chatbots and virtual assistants provide continuous, real-time support across digital channels. In human resources, AI facilitates data-driven decision-making through enhanced candidate matching, streamlined onboarding, and performance monitoring.[287] Operationally, AI enables predictive forecasting, inventory optimization, and real-time analytics, allowing organizations to anticipate demand and allocate resources more efficiently.

The franchise business model illustrates the transformative potential of AI in a particularly acute way. Because franchise systems rely on standardized processes implemented across geographically dispersed, independently owned locations, they present both a challenge and an opportunity for technological integration.[288] AI offers a uniquely powerful mechanism to reconcile these competing demands by enforcing brand-wide consistency while preserving the localized flexibility necessary for franchisee success. Increasingly, franchisors are deploying centralized AI platforms that integrate supply chain management, compliance monitoring, operational guidance, and real-time analytics, ensuring that each franchise location benefits from uniform, data-driven decision-making without requiring duplicative infrastructure or expertise at the unit level.

Importantly, AI's impact in franchising extends beyond internal operations to strategic decision-making at the earliest stages of the business lifecycle. As highlighted in a recent *Franchise Times* report, franchisors are increasingly leveraging AI to identify and evaluate optimal site locations for new units.[289] By aggregating and analyzing vast datasets, including demographic trends, traffic patterns, consumer behavior, competitor

---

[286] Michelle Rowan, *How AI-Enabled Franchise Support Will Redefine Growth, Talent, and Franchisee Success in 2026*, FRANCHISE BUS. REV. (Dec. 11, 2025), https://tour.franchisebusinessreview.com/posts/how-ai-enabled-franchise-support-will-redefine-growth-talent-and-franchisee-success-in-2026/.

[287] *See* Kelley & Rogers, *supra* note 1.

[288] Rachael Nicholson, *AI and Franchising: What Entrepreneurs Need to Know (+ Examples)*, HubSpot (Oct. 3, 2025), https://blog.hubspot.com/sales/ai-franchise.

[289] *Why More Franchises Are Tapping AI to Pinpoint Top Sites*, FRANCHISE TIMES (Oct. 2024), https://www.franchisetimes.com/franchise_operations/why-more-franchises-are-tapping-ai-to-pinpoint-top-sites/article_3325fcb0-8fdd-11ef-bf97-8f3de8a3639a.html.

proximity, and economic indicators, AI-enabled site selection tools can predict with greater precision which locations are most likely to succeed. This represents a significant evolution from traditional, experience-based site selection toward a more empirical, predictive model that reduces risk and enhances system-wide performance. In a franchise context, where location is often determinative of success, this capability alone underscores AI's strategic importance.[290]

At the operational level, AI-driven systems are fundamentally transforming how franchise businesses manage day-to-day execution. Advanced demand forecasting tools synthesize historical sales data, local market dynamics, seasonal trends, and exogenous variables (*e.g.*, weather patterns or regional events) to optimize inventory management, thereby minimizing stockouts while reducing costly overproduction in margin-sensitive environments. Workforce management has undergone a parallel evolution, with dynamic scheduling algorithms that continuously adjust staffing levels based on real-time and predictive demand signals, improving labor efficiency without compromising service quality.[291] These developments are not hypothetical. Recent research highlighted by Deloitte underscores that AI is already reshaping restaurant and service-based franchise operations from "the dining room to the kitchen and drive-thru," with a significant majority of operators increasing investment in AI to enhance both customer experience and operational performance.[292] AI's strength in predictive analytics enables organizations to more precisely align staffing, inventory, and service delivery with anticipated demand, while also unlocking cost efficiencies and improving employee experience through reduced operational friction.[293]

At the customer interface, AI-enabled chatbots, voice assistants, and digital ordering systems deliver consistent, brand-aligned interactions across websites, mobile applications, and in-store platforms, ensuring uniform customer experiences across the franchise network. These tools increasingly support personalization at scale by tailoring recommendations, promotions, and service interactions based on individual consumer data, while also automating high-volume, routine interactions that would otherwise strain human staff. Collectively, these capabilities illustrate how AI is not merely improving discrete operational functions, but rather creating an integrated, data-driven ecosystem that enhances efficiency, consistency, and customer engagement across the entire franchise enterprise.

Franchise systems further leverage AI in ways that directly enhance scalability, representing one of the core economic advantages of the model. In service-oriented sectors such as home services and quick-service restaurants, AI-powered route

---

[290] *Id.*

[291] Bradford J. Kelley, *Wage Against the Machine: Artificial Intelligence and the Fair Labor Standards Act*, 34 STAN. L. & POL'Y REV. 261 (2023).

[292] Deloitte, *Deloitte: Restaurant AI Investments Heat Up, But Adoption Still Appears to Be on the Back Burner* (June 23, 2025), https://www.deloitte.com/us/en/about/press-room/deloitte-how-ai-is-revolutionizing-restaurants.html.

[293] *Id.*

optimization and automated dispatching reduce travel time, lower fuel costs, and improve service responsiveness. At the same time, AI-driven training platforms and virtual assistants enable rapid, standardized onboarding for new franchisees and employees, helping maintain brand integrity even as systems expand quickly across new markets. These tools function not merely as operational enhancements, but as force multipliers that allow franchisors to scale without sacrificing consistency or control.

AI is also transforming franchise marketing by enabling highly targeted, data-driven campaigns that can be deployed consistently across locations while still accounting for local market nuances. As highlighted by the International Franchise Association, franchise service brands are increasingly using AI to analyze customer data, segment audiences, and personalize outreach, thereby allowing franchisors and franchisees to optimize digital advertising spend, refine messaging, and improve customer acquisition and retention in real time.[294] These capabilities allow franchise systems to move beyond static, one-size-fits-all marketing toward dynamic, continuously optimized engagement strategies that scale efficiently across entire networks.[295]

The resulting efficiencies are substantial: in targeted use cases, franchise systems report operational cost reductions of 20–30%, alongside improvements in customer satisfaction and revenue performance. More fundamentally, AI enables franchise owners to shift their focus away from routine administrative burdens and toward higher-value activities such as business development, customer relationships, and strategic growth. In this respect, AI is not merely enhancing the franchise model; it is redefining its competitive advantage in an increasingly data-driven economy.[296]

B. Wyndham Hotels: An Illustration

The deployment of AI within franchise systems is not theoretical; it is already occurring at scale. A particularly instructive example is Wyndham Hotels & Resorts, the world's largest hotel franchising company, which has partnered with PwC to implement agentic AI across its global franchise network.[297] Through this initiative, Wyndham has introduced AI agents designed to serve as a centralized operational interface for franchisees. These systems provide real-time access to brand standards, operational guidance, and compliance resources, effectively functioning as an always-available digital advisor. Franchisees can use these tools to obtain immediate answers to routine operational and compliance questions, while more complex or sensitive issues are

---

[294] Ben Gergis & Justin Waltz, *Tech & Trends: How Franchise Service Brands Are Embracing AI and Revolutionizing Operations*, INT'L FRANCHISE ASS'N (Feb. 20, 2025), https://www.franchise.org/2025/02/tech-trends-how-franchise-service-brands-are-embracing-ai-and-revolutionizing-operations/.

[295] *Id.*

[296] *See* Rowan, *AI-Enabled Franchise Support*, *supra* note 7.

[297] *Wyndham Hotels & Resorts: Transforming Global Operations with AI Agents*, PricewaterhouseCoopers, https://www.pwc.com/us/en/library/case-studies/wyndham-agentic-ai.html.

escalated to human personnel. This hybrid model enhances efficiency while preserving appropriate human oversight.[298]

AI is also transforming Wyndham's customer-facing operations. AI-driven agents now manage a wide range of guest interactions, including reservation modifications, loyalty program inquiries, check-in and check-out processes, and personalized booking assistance.[299] These interactions occur across both chat and voice platforms, often in real time. By automating high-volume, routine inquiries, Wyndham has reduced call center burdens, improved response times, and enhanced overall customer satisfaction, while enabling franchise operators to scale service delivery without proportional increases in staffing.[300]

More broadly, Wyndham's implementation reflects an emerging paradigm in franchise systems: AI as a unifying infrastructure layer. By integrating franchisors, franchisees, employees, and customers through shared data systems and standardized processes, AI enables greater operational cohesion across decentralized networks. At the same time, it reinforces brand consistency, enhances decision-making, and creates new efficiencies that would be difficult to achieve through traditional management structures alone.

III. Legal Risks Associated with AI in the Workplace

A. Employment Law Concerns

Although AI represents a novel set of tools, the conduct it enables is not novel, nor does it exist outside established legal boundaries. U.S. labor and employment law has long regulated discrimination, harassment, retaliation, surveillance, and wage practices without regard to the medium through which those practices occur. AI does not displace these frameworks; rather, it operates squarely within them. The relevant inquiry remains unchanged: whether the employer's conduct, however executed, violates existing statutory or common-law standards.

Federal anti-discrimination laws, including Title VII of the Civil Rights Act of 1964, already prohibit employment practices that result in disparate treatment or disparate impact on protected classes. That prohibition applies with equal force whether decisions are made by a human manager, a rules-based algorithm, or a machine-learning system.[301] For example, the use of AI to generate synthetic or sexually explicit images of a coworker constitutes actionable workplace harassment, no different in kind from

[298] *Id.*

[299] *Id.*

[300] *Id.*

[301] *See* Sonderling, Kelley & Casimir, *supra* note 6.

harassment carried out through traditional means. The technological sophistication of the tool does not alter the legal analysis; the harm and the standard remain the same.[302]

The Americans with Disabilities Act ("ADA") presents a particularly acute area of risk for AI-driven employment tools. Automated screening and assessment systems may unlawfully disadvantage individuals with disabilities when employers rely on proxies that correlate with disability status or penalize atypical modes of communication or behavior.[303] An AI-powered video interview platform that assigns lower scores based on a candidate's failure to maintain eye contact, vocal cadence, or facial expressiveness may disproportionately screen out individuals with autism spectrum disorder, vision impairments, or neurological conditions.[304] Similarly, systems that automatically disqualify applicants based on physical-task assumptions, such as the ability to stand for extended periods, without providing an opportunity to request reasonable accommodation raise serious ADA concerns. AI tools may also implicate the ADA if they infer or detect non-obvious medical conditions. For example, if an algorithm identifies a hand tremor and flags the applicant accordingly, that could constitute a prohibited disability-related inquiry, as tremors may be associated with neurological conditions such as cerebral palsy, Parkinson's disease, or the aftermath of a stroke. In each of these scenarios, existing federal law already provides clear protections and legal remedies.[305] There is no regulatory vacuum; only a need to ensure that employers apply existing laws to emerging technologies with care and diligence. In other words, existing ADA doctrine already addresses these scenarios; the challenge lies in disciplined application, not doctrinal innovation.[306]

AI-enabled workplace monitoring likewise remains governed by longstanding labor law principles, most notably the National Labor Relations Act ("NLRA").[307] Enacted in 1935, long before the advent of modern surveillance tools or artificial intelligence, the NLRA protects employees' rights to engage in concerted activities for mutual aid or protection and prohibits employers from interfering with, restraining, or coercing employees in the exercise of those rights. Whether monitoring is conducted by a supervisor observing the shop floor or by an AI system analyzing communications metadata, productivity metrics, or behavioral patterns, the legal inquiry is identical. AI does not alter these foundational protections; it merely introduces new technological means through which regulated conduct may occur.[308] Whether monitoring is carried out by a frontline supervisor or an algorithmic system, the legal constraints are identical. If AI-enabled surveillance chills protected concerted activity, it raises the same NLRA concerns

---

[302] *See* Kelley & Asghar, *supra* note 4.

[303] *See* Sonderling, Kelley & Casimir, *supra* note 6.

[304] *Id.*

[305] *Id.*

[306] *Id.*

[307] Bradford J. Kelley, *All Along the New Watchtower: Artificial Intelligence, Workplace Monitoring, Automation, and the National Labor Relations Act*, 107 MARQ. L. REV. 195, 198 (2023).

[308] *Id.*

as traditional forms of employer monitoring. The NLRA is technology-neutral, and its protections extend fully to modern AI-enabled management practices. In other words, AI merely introduces new tools to engage in conduct the NLRA has long governed.[309]

Wage-and-hour compliance under the Fair Labor Standards Act ("FLSA") follows the same logic. Employers increasingly rely on AI for timekeeping, scheduling, payroll, and productivity analysis.[310] While the tools may be new, the legal obligations are not. Indeed, the introduction of AI does not diminish the employer's obligation to compensate employees for all hours worked or to comply with overtime and minimum-wage requirements. An AI system that undercounts compensable time does not create a regulatory gap; it creates liability. Properly designed and implemented, AI will ultimately enhance wage and hour compliance by increasing accuracy, consistency, and transparency.[311]

Nor does the use of AI alter the long-established legal standards governing worker classification or joint employer status. While some critics argue that AI-driven management tools such as algorithmic scheduling, productivity monitoring, or automated supervision increase employer control in ways that heightens misclassification risk or joint employment risk, the governing legal tests remain unchanged.[312] Control has always been the touchstone, not the mechanism through which it is exercised. Plus, the criticism misconstrues how AI is deployed in practice. In reality, AI frequently increases worker autonomy by enabling greater scheduling flexibility and operational independence. For instance, AI-enabled platforms can allow workers to choose shifts that align with their preferences, manage their workloads more efficiently, and tailor their schedules around personal responsibilities. Rather than expanding employer control, these systems frequently decentralize it, empowering workers and reinforcing employment models that prioritize flexibility, independence, and fairness.[313]

Federal agencies themselves appear to recognize that the existing legal framework is largely sufficient to address AI-related issues in the workplace. For example, in 2021, the EEOC launched an initiative to ensure that employers' use of AI and other emerging technologies in hiring and employment decisions complies with the federal civil rights laws the agency enforces.[314] However, the initiative has remained largely inactive in recent years, with little public engagement and no new guidance issued.[315] This prolonged dormancy strongly suggests that the EEOC has not identified any novel or unaddressable risks posed by AI that fall outside the scope of existing anti-discrimination

---

[309] *Id.*

[310] Bradford J. Kelley, *Wage Against the Machine: Artificial Intelligence and the Fair Labor Standards Act*, 34 STAN. L. & POL'Y REV. 261 (2023).

[311] *Id.*

[312] *Id.*

[313] *Id.*

[314] *See* Kelley & Rogers, *supra* note 1.

[315] *Id.*

statutes. Rather than indicating a gap in the law, the agency's limited activity reflects a broader institutional understanding that current legal protections remain fully applicable and effective in the face of technological change.

Taken together, these doctrines underscore a central point: the U.S. employment law framework is neither obsolete nor ill-equipped to address AI risks in the workplace. The risks associated with AI in employment arise not from the absence of regulation, but from the scale, speed, and opacity with which traditional employment decisions can now be made. The law already governs the conduct. The imperative for employers is to ensure that AI systems are deployed with appropriate governance, transparency, and human oversight to ensure compliance with longstanding legal obligations.

B. Privacy and Data Protection

The rapid deployment of AI tools in the workplace has dramatically expanded the scope, scale, and sensitivity of employee data collection, intensifying privacy and data-protection risks in ways that traditional employment practices did not.[316] Modern AI systems routinely ingest, process, and retain large volumes of personal information, including biometric identifiers (such as facial geometry, voiceprints, and keystroke dynamics), behavioral and productivity metrics, geolocation data, and the content of written and oral communications. Unlike conventional human resource systems, these tools often operate continuously, passively, and at scale, aggregating data over time to generate inferences about employees and applicants that may extend well beyond the original purpose of collection.

One of the most acute privacy risks arises from AI-enabled monitoring and surveillance. Employers increasingly rely on AI to assess productivity, engagement, safety, and collaboration by analyzing communications metadata, screen activity, location data, and audio or video feeds. Although workplace monitoring is not new, AI dramatically increases its granularity, persistence, and intrusiveness, raising questions about notice and consent.[317]

AI-powered transcription and meeting-assistant tools present a distinct and rapidly expanding risk profile. While such tools promise efficiency gains through automated note-taking and documentation, they also implicate federal and state wiretap statutes, many of which prohibit the interception or recording of communications without proper consent.[318] In all-party consent jurisdictions such as California and Illinois, the unauthorized recording of meetings, whether virtual or in person, can expose employers to significant statutory damages, class-action litigation, and injunctive relief.

---

[316] Zoe Argento & Bradford Kelley, *AI Transcription and Note-Taking Technologies: Seven Points for Employers to Consider*, LITTLER (Feb. 26, 2026), https://www.littler.com/news-analysis/asap/ai-transcription-and-note-taking-technologies-seven-points-employers-consider.

[317] *Id.*

[318] *Id.*

Beyond consent issues, transcription tools frequently capture highly sensitive information, including attorney-client communications, medical disclosures, trade secrets, and internal deliberations. The downstream risks are substantial. Recorded content may be stored indefinitely, processed outside the employer's control, or used to train vendors' machine-learning models, raising concerns about privilege waiver, confidentiality breaches, and secondary data use. These risks are not hypothetical; recent litigation has squarely challenged whether AI transcription providers unlawfully intercept communications and repurpose captured data without adequate disclosure or authorization.

IV. The Evolving Regulatory Landscape

While existing employment laws largely govern the conduct enabled by AI, state and local governments have increasingly pursued AI-specific regulation aimed at employment decision-making.[319] These efforts reflect growing political and public concern about algorithmic opacity, bias, and accountability. Yet the resulting regulatory framework is highly fragmented, unevenly enforced, and, in many cases, internally inconsistent. For employers operating across multiple jurisdictions, the practical challenge is not the absence of law, but the proliferation of overlapping and sometimes ill-defined obligations layered atop already robust, technology-neutral legal regimes.

Rather than creating a unified national standard, states and municipalities have adopted divergent approaches that vary significantly in scope, terminology, enforcement mechanisms, and compliance burdens. As a result, employers must navigate a complex patchwork that often prioritizes process over outcomes and symbolism over functional risk reduction.

A. New York City Local Law 144

New York City's Automated Employment Decision Tools Law ("Local Law 144"), enacted in 2021 and effective July 2023, was the first comprehensive U.S. law to regulate AI-assisted hiring and promotion decisions.[320] The statute requires covered employers and employment agencies to conduct annual independent bias audits of automated employment decision tools, publicly post a summary of audit results, and provide advance notice to affected candidates.[321]

Despite its ambitious goals, it has been widely criticized for vague definitions, limited enforcement, and minimal practical impact. Key statutory terms, including what qualifies as an "automated employment decision tool," what constitutes "substantial assistance" by such a tool, and how bias audits should be conducted, remain imprecise. The result has been widespread uncertainty among employers and auditors alike, undermining meaningful compliance. A *Law360* article entitled, "'*Everyone Ignores' New*

[319] *See generally* Sonderling, Kelley & Casimir, *supra* note 6.

[320] *Id.*

[321] *Id.*

York City's Workplace AI Law" reported that most practitioners view the law as a "toothless flop" and highly ineffective.[322] Similarly, the Society for Human Resource Management, the world's largest professional HR association, published an article titled, "*New York City AI Law is a Bust*" explaining that the law has failed to deliver on its promises.[323]

Empirical evidence confirms these concerns. A 2024 Cornell University study found that the overwhelming majority of New York City employers were not complying with the law's audit and notice requirements. Subsequent reporting and a December 2025 audit by the New York State Comptroller further criticized the Department of Consumer and Worker Protection for ineffective enforcement, citing superficial compliance reviews, poor complaint handling, and a lack of proactive oversight.[324] In practice, Local Law 144 has become emblematic of a broader problem in AI regulation: ambitious statutory design paired with weak execution and limited real-world effect.

B. Illinois Artificial Intelligence Laws

Illinois has adopted a more aggressive and comprehensive approach to regulating AI in employment. The Artificial Intelligence Video Interview Act requires employers to notify applicants when AI is used to evaluate video interviews, explain how the technology works, and obtain consent prior to use. More significantly, amendments to the Illinois Human Rights Act enacted through HB 3773, effective January 1, 2026, explicitly prohibit the use of AI in recruitment, hiring, promotion, discipline, and other employment decisions if it results in discrimination against protected classes, even absent intent. The law also imposes certain notice requirements.

Draft regulations from the Illinois Department of Human Rights further clarify notice obligations and reinforce anti-discrimination standards. When combined with the state's Biometric Information Privacy Act, Illinois now imposes some of the most stringent compliance obligations in the country, particularly for AI tools involving biometric data such as facial recognition, voice analysis, or video-based assessments.

For multi-state employers, Illinois illustrates both the promise and peril of AI-specific legislation. While the framework provides clearer substantive standards than Local Law 144, it also significantly raises compliance stakes and litigation exposure.

C. Colorado AI Act

Colorado's Artificial Intelligence Act aims to impose risk-management, impact-assessment, and disclosure obligations on developers and deployers of "high-risk" AI systems affecting consequential decisions, including employment. Enacted in 2024 through an accelerated legislative process designed to outpace the European Union's AI

---

[322] *See* Kelley & Rogers, *supra* note 1.

[323] *Id.*

[324] *Enforcement of Local Law 144 on Automated Employment Decision Tools*, N.Y. Off. of the State Comptroller (Dec. 2, 2025), https://www.osc.ny.gov/state-agencies/audits/2025/12/02/enforcement-local-law-144-automated-employment-decision-tools.

Act, Colorado Senate Bill 24-205 was passed before foundational elements of its regulatory framework were fully developed.[325] The result is a law so riddled with ambiguity and drafting flaws that, on the very day of signing, the governor publicly expressed "reservations" about its provisions and called on the legislature to "fine tune" the statute. Shortly thereafter, the governor, state attorney general, and state senate majority leader authored an open letter to the business community to "provide additional clarity" and committed to "engage in a process to revise the new law" and "minimize unintended consequences associated with its implementation."[326] In effect, Colorado enacted a regulatory regime with the full expectation that it would need to be rewritten before taking effect, leaving employers in limbo and state agencies uncertain about how, or even whether, to implement the law as written.

D. California's Emerging Regulatory Framework

California is advancing a more incremental but expansive approach to regulating AI in employment by clarifying that existing anti-discrimination law applies fully to automated decision systems. In October 2025, the California Civil Rights Department issued regulations under the Fair Employment and Housing Act expressly confirming that AI-driven systems, including algorithms, machine learning models, and automated decision tools, are subject to the same disparate treatment and disparate impact standards as human decision-makers. Rather than creating a standalone AI statute, California's approach reinforces the technology-neutral nature of civil rights law while signaling aggressive enforcement expectations.

Taken together, these regulatory developments reflect a broader trend toward AI-specific oversight without consensus on form or function. For employers, particularly franchisors and other scalable business models, the challenge is not simply legal compliance, but operational coherence. Divergent state and local regimes create incentives to adopt the most restrictive standards nationwide, effectively allowing the most aggressive jurisdiction to set the baseline for all operations.

Critically, none of these frameworks displace existing federal employment law. Instead, they layer procedural obligations such as audits, notices, disclosures, and impact assessments, on top of longstanding substantive standards. As a result, the primary risk for employers lies not in novel legal theories, but in failure to implement disciplined governance, documentation, and oversight capable of withstanding scrutiny across jurisdictions.

V. Key Litigation Developments

Recent litigation has begun to define the contours of liability for AI-driven employment practices, testing how longstanding statutory frameworks apply to algorithmic decision-making at scale. While courts have not articulated a standalone body

[325] *Id.*

[326] *Id.*

of “AI employment law,” plaintiffs are increasingly deploying creative theories under existing anti-discrimination, privacy, and consumer-protection statutes to challenge both employers and technology vendors. These cases underscore a central theme: AI does not create new legal obligations, but it can dramatically amplify exposure by accelerating, systematizing, and obscuring traditional employment decisions.

A. Vendor Liability: *Mobley v. Workday, Inc.*, 3:23-cv-770 (N.D. Cal. filed Feb. 21, 2023)

Mobley v. Workday, Inc., No. 3:23-cv-00770 (N.D. Cal., filed Feb. 21, 2023), stands as a landmark case testing the boundaries of vendor liability under federal employment discrimination statutes. Plaintiffs, including lead plaintiff Derek Mobley, claim that Workday’s AI-powered applicant screening, scoring, ranking, and recommendation tools systematically disadvantaged candidates on the basis of race, age, and disability. The plaintiffs allege that the system relied on biased training data and proxy variables, resulting in rapid rejections for hundreds of qualified applications.

Plaintiffs advance that Workday functions as an “agent” of its employer-customers by exercising delegated authority over key aspects of the hiring process, thereby subjecting the software vendor itself to liability under Title VII of the Civil Rights Act of 1964, the Age Discrimination in Employment Act, and the Americans with Disabilities Act. The case also asserts both disparate treatment and disparate impact theories.

B. An Employer’s Use of AI Tools: *Harper v. Sirius XM Radio, LLC*, 2:25-cv-12403 (E.D. Mich. Filed Aug. 4, 2025)

Harper v. Sirius XM Radio, LLC, No. 2:25-cv-12403 (E.D. Mich., filed Aug. 4, 2025), is a proposed class action that illustrates the growing risk of employment discrimination claims arising from AI-powered resume screening tools. Plaintiff Arshon Harper, an African American IT professional, alleges that Sirius XM’s use of a third-party AI-driven applicant tracking system, specifically the iCIMS platform, systematically disadvantaged Black applicants by perpetuating historical biases embedded in the tool’s training data.

According to the complaint, Harper applied to approximately 150 positions for which he was qualified yet received only one interview. The suit asserts claims of both disparate treatment and disparate impact under Title VII of the Civil Rights Act of 1964 and 42 U.S.C. § 1981. Harper contends that the AI system assigned lower scores or automatically filtered out candidates based on proxy variables strongly correlated with race, including educational institutions attended, employment history gaps, residential zip codes, and other socioeconomic indicators. These factors, the complaint alleges, caused the algorithm to “learn” and replicate past discriminatory hiring patterns rather than evaluate applicants solely on job-related criteria.

Harper v. Sirius XM reinforces a critical lesson: algorithmic hiring tools are fully subject to Title VII’s prohibitions on both intentional and unintentional discrimination. Employers and franchisors that fail to audit these systems for proxy-based bias risk not

only individual lawsuits but also broader enforcement actions and reputational damage across the entire brand.

C. Privacy, Surveillance, and Consent-Based Claims: *In re Otter.AI Privacy Litigation*, 5:25-cv-6911 (N.D. Cal. filed Aug. 15, 2025)

In re Otter.AI Privacy Litigation, No. 5:25-cv-6911 (N.D. Cal., filed Aug. 15, 2025), is a consolidated putative class action that has emerged as a leading case addressing privacy risks associated with AI-powered workplace monitoring and transcription tools. Originally filed as *Brewer v. Otter.AI, Inc.* and later consolidated with related actions, the litigation alleges that Otter.ai's popular AI meeting assistant unlawfully records, intercepts, and processes private conversations during virtual meetings.

Plaintiffs contend that the tool automatically joins meetings (sometimes as a "silent participant"), captures audio in real time, transmits content to Otter's servers, and uses the resulting transcripts and recordings to train the company's machine-learning and automatic speech recognition models—often without meaningful notice to or consent from all participants, including non-Otter users. The consolidated complaint asserts claims under the federal Electronic Communications Privacy Act, the California Invasion of Privacy Act, the Computer Fraud and Abuse Act, and related state statutes, including allegations of wiretapping violations and unfair business practices.

D. Government Enforcement: *EEOC v. iTutorGroup, Inc.*, No. 1:22-cv-02565 (E.D.N.Y.)

EEOC v. iTutorGroup, Inc., No. 1:22-cv-02565 (E.D.N.Y. filed May 5, 2022), represents one of the EEOC's earliest enforcement actions challenging algorithmic discrimination in hiring. The agency alleged that iTutorGroup, an online English-language tutoring provider, programmed its recruitment software to automatically reject female tutor applicants age 55 and older and male applicants age 60 and older. This hardcoded age- and sex-based filtering resulted in the automatic exclusion of more than 200 otherwise qualified U.S.-based applicants during a brief 2020 hiring window.

The case settled in 2023 via consent decree approved on September 8, 2023. Without admitting liability, iTutorGroup agreed to pay $365,000 to be distributed among affected applicants.[327] The decree also imposed significant injunctive relief, including a prohibition on requesting applicants' dates of birth prior to a conditional job offer; bans on screening or rejecting applicants based on age or sex; development and distribution of revised anti-discrimination policies and complaint procedures; mandatory training for personnel involved in hiring; and ongoing EEOC monitoring. Because iTutorGroup had ceased U.S. hiring operations by the time of settlement, the injunctive provisions apply for five years from the decree's effective date or three years after any resumption of hiring,

[327] *iTutorGroup to Pay $365,000 to Settle EEOC Discriminatory Hiring Suit*, U.S. Equal Emp. Opportunity Comm'n (Sept. 11, 2023), https://www.eeoc.gov/newsroom/itutorgroup-pay-365000-settle-eeoc-discriminatory-hiring-suit.

whichever is longer. The company must also notify previously rejected applicants and afford them priority consideration should hiring resume.

Although the settlement was reached in 2023, the case remains highly instructive. It marked an early demonstration of the EEOC's commitment to scrutinizing automated hiring tools under the Age Discrimination in Employment Act and signaled the agency's broader Artificial Intelligence and Algorithmic Fairness Initiative. The settlement underscores that even straightforward algorithmic filters can trigger liability when they embed protected-class criteria or produce clear disparate treatment.

E. Transparency, Consumer Reporting, and Novel Theories: *Kistler et al. v. Eightfold AI Inc.*, No. C26-00214 (Cal. Super. Ct., removed to N.D. Cal. 3:26-cv-01768)

Kistler et al v. Eightfold AI Inc., filed January 20, 2026, in California Superior Court (Contra Costa County, No. C26-00214) and later removed to the Northern District of California (No. 3:26-cv-01768), represents a novel class action that shifts the focus from algorithmic bias to transparency and consumer-protection obligations in AI-driven hiring. Plaintiffs allege that Eightfold's talent intelligence platform scrapes vast amounts of personal data to build detailed applicant profiles and generate proprietary "Match Scores" based on extensive data aggregation and that employers rely on those scores to rank and automatically filter candidates without disclosure or opportunity for review.

Rather than alleging discriminatory outcomes, the complaint asserts that Eightfold functions as a consumer reporting agency under the Fair Credit Reporting Act and analogous state statutes. The suit asserts that Eightfold failed to provide required disclosures, obtain authorizations, or afford applicants the opportunity to review, dispute, or correct the information. As of March 2026, the case remains in its early stages. This litigation reflects an emerging plaintiff strategy to regulate AI employment tools through longstanding consumer-protection statutes rather than anti-discrimination laws.

Taken together, these cases reveal a consistent judicial trajectory. Courts and regulators are not carving out special exemptions, or special rules, for AI. Instead, they are applying existing statutes to new technological contexts, often with heightened sensitivity to scale, delegation, and opacity.

VI. Recommended Practices for Employers

In light of the expanding and increasingly fragmented regulatory landscape, coupled with a growing wave of litigation targeting AI-driven employment practices, employers must move beyond reactive, tool-specific compliance and adopt comprehensive, enterprise-wide governance strategies. The central risk associated with workplace AI is not the novelty of the technology itself, but the scale, opacity, and speed with which employment decisions can now be made. Effective risk mitigation therefore requires structures that emphasize accountability, transparency, and disciplined human oversight. Recommended practices must be designed not merely to satisfy individual statutes, but to withstand scrutiny across jurisdictions, regulators, and litigation forums.

A. Establishing Comprehensive AI Governance Frameworks

Employers should implement a formal, written AI policy as the foundation of any responsible workplace AI strategy. An AI policy is not merely a compliance document; it is a governance instrument that establishes enterprise-wide guardrails for how AI tools are selected, deployed, monitored, and relied upon in employment-related decisions.[328] In the absence of a defined framework, employees and business units may adopt AI technologies in inconsistent, ad hoc, or unauthorized ways, thereby creating significant exposure to discrimination claims, privacy violations, confidentiality breaches, and overreliance on inaccurate or unvalidated outputs. A well-constructed AI policy enables employers to identify and categorize high-risk use cases, particularly those involving employment decision-making, while clearly delineating permissible and prohibited applications and ensuring alignment with a rapidly evolving and increasingly complex regulatory landscape.

Beyond risk mitigation, AI policies serve as the backbone of a broader governance architecture that promotes accountability, consistency, and control across the enterprise. Effective policies establish centralized processes for vendor selection and oversight, data governance and security, and model validation and monitoring. Critically, they also formalize the role of human oversight in AI-assisted decision-making, requiring appropriate review, escalation protocols, and documentation where AI outputs may affect hiring, discipline, compensation, or termination decisions. By clearly defining expectations, including limitations on data inputs, requirements for transparency and explainability, and standards for validating AI-generated outputs, employers can reduce implementation variability, enhance auditability, and strengthen defensibility in the face of regulatory scrutiny or litigation. Documenting these processes is critical. In litigation and enforcement actions, the ability to demonstrate structured oversight often matters as much as the underlying technical design of the tool itself.

In this respect, an AI policy is not merely a compliance instrument, but a strategic governance tool. It enables organizations to harness the benefits of AI while embedding safeguards that preserve human judgment, protect employee rights, and ensure that technological innovation remains aligned with legal obligations and core business values.

B. Bias Audits

Employers should conduct periodic, defensible bias and impact assessments of AI tools used across the employment lifecycle. These assessments should go beyond superficial box-checking exercises and instead evaluate how tools perform in practice, including whether they disproportionately affect protected classes under disparate impact standards. Best practice assessments typically involve testing AI systems against historical and synthetic datasets, evaluating selection rates and impact ratios, and examining proxy variables that may correlate with protected characteristics. Where

[328] Bradford J. Kelley, Michael Skidgel, & Alice Wang, *Considerations for Artificial Intelligence Policies in the Workplace*, LITTLER (Mar. 10, 2025), https://www.littler.com/news-analysis/asap/considerations-artificial-intelligence-policies-workplace.

disparities are identified, employers should be prepared to take documented remedial action such as modifying inputs, adjusting thresholds, increasing human review, or discontinuing use altogether.

Equally important is recordkeeping. Employers should maintain detailed documentation of audit methodologies, findings, and corrective measures, and retain those records for extended periods. As recent litigation illustrates, the absence of documentation can itself become a source of liability, particularly where plaintiffs allege opacity or lack of oversight.

C. Transparency

Employers should strive to be transparent with their use of AI. Employers should provide clear, timely, and meaningful notice to applicants and employees when AI tools are used to inform or influence decisions related to recruitment, screening, promotion, discipline, or termination. At a minimum, such notices should explain the purpose of the AI system, the types of data it collects and analyzes, the nature of its role in the decision-making process, and the extent to which human oversight is involved. Boilerplate or overly technical disclosures are insufficient; effective transparency requires information that is understandable, accessible, and tailored to the specific use case.

Regulators are increasingly codifying these expectations. For example, the new Illinois AI law and similar state measures impose explicit notice and disclosure obligations tied to the use of AI in employment decisions, reflecting a broader trend toward mandated transparency and accountability. However, recommended practices extend beyond minimum legal requirements. Employers should consider implementing enhanced transparency measures, such as providing advance notice prior to AI-assisted evaluations, offering applicants and employees the opportunity to request human review or alternative assessment methods, and maintaining accessible channels for questions or challenges to AI-driven outcomes.

From a risk-management perspective, transparency serves multiple functions: it supports compliance with emerging legal standards, mitigates potential claims of unfairness or deception, and builds trust among employees and applicants. In an environment where AI systems may otherwise appear opaque or “black box” in nature, meaningful transparency helps ensure that individuals understand how decisions are made and reinforces the legitimacy of the employer’s processes.

D. Vendor Due Diligence and Oversight

Reliance on third-party vendors does not insulate employers from liability associated with AI-driven employment tools. To the contrary, courts and regulators are increasingly scrutinizing whether vendors function as agents of the employer, particularly where their technologies materially influence employment decisions. As a result,

franchisors and franchisees must treat vendor selection and oversight as a critical component of their overall risk management strategy, rather than a delegable function.[329]

At a minimum, employers should conduct thorough, documented due diligence before engaging any AI vendor, including evaluating the tool's design, data sources, validation processes, and susceptibility to bias or error. Contractual agreements should include robust protections, such as representations and warranties regarding legal compliance, obligations to conduct and share bias audits, data security and confidentiality provisions, clear limitations on data use (including restrictions on model training), and indemnification clauses addressing potential claims arising from the vendor's technology. Ongoing monitoring is equally important; employers should periodically reassess vendor performance, compliance posture, and alignment with evolving legal standards.

E. Embrace Self-Regulation and Leverage Industry Guidance

In the absence of a comprehensive and uniform federal framework governing workplace AI, employers should adopt a proactive self-regulatory approach grounded in recognized industry standards and evolving best practices.[330] Waiting for regulatory clarity is neither practical nor defensible in an environment where enforcement activity and private litigation are already accelerating. Instead, employers should look to credible industry organizations and thought leaders to inform internal governance structures, risk mitigation strategies, and operational safeguards.[331]

The IFA provides a useful model in this regard. Through its publications, legal symposiums, and practitioner-focused resources, the IFA has developed and disseminated practical guidance on the responsible use of AI in franchise systems, including recommendations related to data governance, system-wide consistency, training, and oversight. While not binding, these resources reflect an emerging industry consensus and can serve as persuasive evidence of reasonableness in the event of regulatory scrutiny or litigation. Employers that align their practices with such guidance are better positioned to demonstrate diligence, reduce risk, and maintain credibility with regulators, courts, and stakeholders.

Ultimately, effective self-regulation is not a substitute for compliance, but a necessary complement to it. Organizations that proactively establish internal standards and leverage reputable industry guidance will be better equipped to navigate legal uncertainty, adapt to evolving requirements, and responsibly integrate AI into the employment lifecycle.

---

[329] *See* Sonderling, Kelley & Casimir, *supra* note 6.

[330] *See* Keith E. Sonderling & Bradford J. Kelley, *Filling the Void: Artificial Intelligence and Private Initiatives*, 24 N.C. J. L. & TECH. 153, 161 (2023).

[331] *Id.*

F. Continuous Monitoring and Adaptive Compliance

As the legal and regulatory landscape governing workplace AI continues to evolve at a rapid pace, employers must adopt a proactive and dynamic approach to compliance. This requires not only tracking developments across federal, state, and local jurisdictions, but also continuously assessing how new laws, regulations, and enforcement priorities affect existing AI tools, policies, and operational practices. Static compliance models are insufficient in this environment; instead, employers should implement ongoing monitoring mechanisms to ensure that AI deployments remain aligned with current legal requirements and emerging best practices.

For multi-state and national franchise systems, the challenge is even more pronounced. The patchwork of overlapping and sometimes conflicting regulatory regimes necessitates a coordinated, system-wide strategy. In many cases, the recommended practice is to identify and adopt the most stringent applicable standards, such as those relating to bias auditing, notice and consent, or data governance, and implement them across the network to create a uniform baseline of compliance. This approach not only reduces the risk of jurisdiction-specific violations, but also enhances operational consistency, simplifies training and oversight, and strengthens the organization's ability to defend its practices in the face of regulatory scrutiny or litigation.

Ultimately, continuous adaptation is not merely a compliance necessity, but a strategic imperative. Employers that actively monitor and respond to regulatory developments will be better positioned to mitigate risk, maintain operational agility, and demonstrate leadership in the responsible and lawful use of AI in the workplace.

VII. Conclusion

AI is no longer an emerging concept in the employment context; it is an operational reality reshaping how organizations recruit, manage, and retain their workforces. For employers and franchise systems in particular, AI offers powerful tools to enhance efficiency, consistency, and scalability across decentralized operations. At the same time, the rapid deployment of AI has intensified legal scrutiny, exposing employers to expanding risks related to discrimination, privacy, transparency, and vendor accountability.

As this Article demonstrates, these risks do not arise from a regulatory vacuum. Longstanding, technology-neutral employment laws, including federal anti-discrimination statutes, wage and hour requirements, labor protections, and privacy frameworks, already govern much of the conduct enabled by AI. What is changing is not the legal standard, but the speed, scale, and opacity with which employment decisions can now be made. Layered atop these existing obligations is an increasingly fragmented patchwork of state and local AI-specific regulations and a growing body of litigation testing novel theories of liability against both employers and technology vendors.

In this environment, reactive compliance is insufficient. Employers must adopt deliberate, enterprise-wide strategies that integrate legal compliance, technological oversight, and organizational governance. This includes implementing comprehensive AI

governance frameworks, conducting meaningful bias and risk assessments, ensuring transparency and human oversight in AI-assisted decision-making, and rigorously vetting and monitoring third-party vendors. For franchise systems operating across multiple jurisdictions, the need for a coordinated, system-wide approach is especially acute.

Ultimately, AI's role in the workplace will continue to expand, regardless of regulatory uncertainty or litigation risk. Employers that approach AI thoughtfully will be best positioned to harness its benefits while mitigating exposure. Those that fail to do so risk not only legal liability, but also erosion of trust, brand integrity, and long-term competitiveness. The challenge moving forward is not whether to use AI in employment, but how to do so responsibly, lawfully, and strategically.

International Franchise Association
58th Annual Legal Symposium
May 17-19, 2026

International – Update on China

Dominic Hui
Ribeiro Hui
Shanghai, China

IFA 58th ANNUAL LEGAL SYMPOSIUM

JUDICIAL UPDATE 2026: CHINA

A. CHINA: THE MARKET

Quick Facts (2025)[332]

Population	1,408,280,000
Urban/rural population ratio	67:33
Cities with more than 5 million people	91 (2021 data)
Employed persons	734,390,000
Average wage	¥RMB 124,110/year ($USD17,993.48 /year[333])

Twenty years ago, franchising in China was dominated almost entirely by brands originating from the United States or other foreign countries. In the last 10 years, local Chinese brands have been emerging at an incredible speed. Foreign brands in China are now facing strong competition from local competitors, with Chinese brands demonstrating particular strength in terms of quality, variety, localization334 and price335. Notably, many of the managerial team members of these domestic brands were previously trained by American franchisor personnel. At the same time, many of the new domestic brands are funded by Chinese and foreign sources of private capital targeting higher returns from investment at the early development stage, including a focus on being listed publicly on an accelerated timeline.

Another ongoing trend within China is the emergence of large, sophisticated, capitalized franchisee conglomerates who engage with American franchisors to acquire the rights to all of China or relatively large geographical regions instead of just one to two cities or provinces.

---

[332] National Bureau of Statistics of China, *China Statistical Yearbook 2025*, https://www.stats.gov.cn/sj/ndsj/2025/indexeh.htm (2025), except source of item 3 is Xiaozhao Lin, *Chinese Cities Big Data*, Yicai (第1财经), September 2, 2021, https://news.cctv.com/2021/09/02/ARTILECwFUKLnAj82ybcnk1k210902.shtml.

[333] Exchange rate as of March 2026: ¥RMB 6.90 to $USD1.00.

[334] Luckin Coffee's Moutai (Chinese spirit) latte launched in 2023 remains a very good example of localization of non-Chinese-originated products.

[335] Using a quick example, in Shanghai, the price of a tall latte at an American coffee brand franchised outlet is ¥RMB33 (dine in or paper cup) or ¥RMB29 (bring your own cup); and the price of a cup of latte of comparable size at a Chinese brand franchised outlet is ¥RMB 20 (dine in or paper cup) or ¥RMB15 (bring your own cup).

With competition within China this fierce, especially in the category of retail franchises, turnover rates are high as there is constant influx of new concepts replacing those which become stale or outdated quickly[336].

The food and beverage category ("F&B") continues to attract the largest interest ahead of different types of franchised businesses. The two charts below reflect this market distribution[337], and the dominance of the F&B sector among franchises in China.

The "Two Congresses" were hosted in Beijing in March 2026. The Government has been reassuring the healthy development of private sector economic shall continue after the implementation of the *Private Economy Promotion Law* in 2025.

B. JUDICIAL UPDATE - INTRODUCTION

Franchise lawyers in China were kept busy during 2025. Although there were no new laws and regulations passed by the federal Ministry of Commerce ("MOFCOM") specific to franchising, there were several legislative developments which do impact on aspects of franchise operations, including:

a. Food Supply Chain Management;

b. Pre-paid Cards and Pre-payment schemes;

c. Safe Harbour Rules under Anti-Monopoly Law;

d. 2025 Anti-Unfair Competition Law Amendments;

e. New Law on Commercial Mediation; and

f. 2025 Arbitration Law Amendments.

C. FOOD SUPPLY CHAIN MANAGEMENT

As in the United States, the introduction of central kitchens, outsourced kitchens, dark kitchens, ghost kitchens and cloud kitchens since the COVID-19 pandemic have disrupted conventional F&B franchise operations in China. In the last few years, many

336 For example, a few years ago, small kiosk-size stores with low upfront investment and a focus on delivery apps replaced large, dine-in beverage concepts. In recent years, models such as "low-franchise-fee with high reliance on supply chain profits" (e.g., MIXUE Ice Cream & Tea) have emerged.

337 Hong Can Business Research Institute (红餐产业研究院), *2026 White Paper on Development of Chinese Chain Stores and Franchise Businesses*, at p.7, https://www.canyin88.com/research/detail/2026/0127/323.html (2026).

restaurant chains in China have moved towards pre-made dishes[338] to save costs and utilize experienced cooking staff at outlets.

Generally speaking, franchisees or outsourced kitchens are expected to observe the recipes, standard operation procedures, and approved list of ingredients determined by the franchisor. Notwithstanding that the relevant national standard on food safety in respect of food production[339] has been in place since 2013, we have seen common operational issues in recent years despite such requirements, including:

- Sourcing of ingredients - franchisees or outsourced kitchens may attempt to deviate from using the franchisor's approved ingredients and suppliers, often in an effort to reduce costs. In many cases, ingredients from unapproved sources could be of inferior quality or simply inappropriate for the menu.
- Storage and use of ingredients - some kitchens may be storing food improperly or using expired ingredients.
- Use of unapproved additives, preservatives, and certain prohibited substances.
- General hygienic standards may not be followed.
- Storage and transportation of products - time, storage and transportation conditions (temperature, humidity, etc.).
- Incomplete records of food safety incidents.

1. Rules of Supervision and Management of Food Production Outsourcing (the "Outsourcing Rules"), to be implemented on December 1, 2026

The Outsourcing Rules expressly apply to the outsourcing of food production in franchising[340], including the designation of a local factory to produce food products bearing the franchisor's trademark. The Outsourcing Rules do not specifically define what constitutes an outsourcing party, but the language is broad enough to likely capture F&B franchisors who have engaged domestic producers. The Outsourcing Rules specifically stipulate that franchisors or trademark licensors are not relieved of food safety liability, nor can such a relationship be relied upon as a defence to allegations of food safety violations by the producer [341].

Outsourcing parties are now required to keep records of the qualifications and capability of third party products of food products[342]. A contract should be signed with the essential details of the outsourcing expressly set out[343]. The executed outsourcing

---

[338] See report by Shuchun Zhou, *Xibei PR disaster a blessing in disguise for food industry*, October 15, 2025, China Daily, https://www.chinadaily.com.cn/a/202510/15/WS68eee72ea310f735438b5038.html.
[339] GB 14881-2013, *National Standard of Food Safety – General hygienic standards for food production* (2013).
[340] Article 2.
[341] Article 9.
[342] Article 8.
[343] Article 9.

agreement must be reported to the local Administration of Market Regulation within 10 business days of signing, as well as ongoing reporting of any changes[344].

The outsourcing party is under a general duty to supervise[345], and is now vested with audit rights, notwithstanding although the Outsourcing Rules constitute administrative law, rather than civil law. Such audit rights cover records regarding ingredients acquired by the contractor[346]. The outsourcing party may appoint a representative or a service provider as a stationed onsite supervisor. The records of inspections and audits should be maintained[347]. The objective of the authority in this respect appears to be that the parties ensure that onsite supervisors are stationed at the most important production locations .

The Outsourcing Rules also impose obligations for both parties to maintain records – for products with an expiry date, the records and samples should be maintained at least 6 months after the expiry date, and for those without an expiry date, the records and samples should be kept at least 2 years after the production of the last batch of products[348].

In the event of discovery of potential or actual food safety incidents, the contractor should immediately cease any production and a report should be made to the local Administration of Market Regulation[349]. Product recall should be arranged accordingly[350]. As this would mean a franchisor would be liable under the Outsourcing Rules for all food safety issues caused by the Chinese producer, the contract should be explicitly clear with respect to that producer's obligations.

2. Local rules and standards in respect of Pre-made Dishes

Pre-made dishes became a controversial issue in late 2025 when consumers in China realized that many of the restaurants they patronized no longer cooked at the restaurant, and many items were merely reheated[351]. Pre-made dishes are defined by the National Administration of Market Regulation as pre-made and pre-packed dishes, using agricultural products and other ingredients, with or without seasonings and without food preservatives, and cooked through industrial process (e.g. stirring, marinating, rolling pressing, frying, deep frying, steaming, etc), with or without seasoning packets, and requiring heating or cooking before consumption. The staple foods, cleaned and cut fresh

[344] Article 10. Changes as to the names, addresses, persons in charge and contact details of both parties to the outsourcing agreement, food production and operation license or registration number for the sale of prepackaged food only, food category, applicable standards, contract term, etc. should be reported.
[345] Article 6.
[346] Article 11.
[347] Article 14.
[348] Articles 12 and 16.
[349] Articles 15 and 17.
[350] Article 17.
[351] See footnote 338.

produce (ready-to-cook vegetables), ready-to-eat foods, or dishes prepared by central kitchens are not included352. In fact, apart from a high-level circular issued by the National Administration of Market Regulation in 2024353, various local rules were issued regarding this growing phenomenon even before the controversies started. Meanwhile, the use of outsourced kitchens or factories is subject to the National Food Safety Standards for Pre-made Dishes.

Essentially, the effect of these changes is to mirror national standards at the level of local rules, including those relating to hygienic requirements354, the use of additives355, and storage and transportation of pre-made dishes. Similar to the Outsourcing Rules, there are also requirements on record keeping and sample retention356, and even ingredients tracing system357.

The operation of central kitchens is subject to another national standard. By definition, a central kitchen is a facility established by a food business enterprise, which centrally processes and produces finished or semi-finished food products for its own chain stores for further processing and dealing before being provided to consumers[358]. Likewise, such set of standards also set out similar food safety and hygienic requirements.

3. Catering Chain Operation Food Safety Corporate Liability Supervision Management Regulations (the "Corporate Liability Regulations")

The Corporate Liability Regulations itself do not impose many new requirements on food safety than those already set out above or otherwise provided for in existing regulations and national standards. Notably, however, the Corporate Liability Regulations

---

352 See *National Food Safety Standards for Pre-made Dishes (Draft for Public Comments)* which was released by the National Food Safety Standards Review Committee on February 6, 2026 (2026). The public consultation period will end on April 8, 2026, and it is expected that the final version of the standards will be issued shortly thereafter,
https://www.nhc.gov.cn/sps/c100087/202602/895e1a278b3b4a3dad3292314770ace5.shtml.

353 Guo Shi Jian Shi Shan Fa (2024) No.27, *Circular on Enhancing the Safety Supervision of Pre-made Dishes and Promoting high quality development*, jointly issued by National Administration of Market Regulation and several administrative agencies (2024).

354 GB 14881-2013, *National Standard of Food Safety – General hygienic standards for food production* (2013).

355 GB 2760-2014, *National Standard of Food Safety – Standard on use of food additives* (2014).

356 Example is Articles 35 and 39 of *Circular on Shandong Province Pre-made Dishes and Food Production Permission Examination Rules* (2025).

357 Example is Article 37 of *Circular on Shandong Province Pre-made Dishes and Food Production Permission Examination Rules* (2025).

358 GB/T 44141-2024, *Central Kitchen -Specifications for Operational and Management* (2024).

require "chain store corporate headquarters" (which may include franchisors) to be responsible for the supervision of ensuring that franchisees comply with these requirements and be liable in the event of failing to supervise[359]. Chain store corporate headquarters cannot waive or be released from these responsibilities and liabilities by way of contract[360].

The Corporate Liability Regulations contain the following definitions which are relevant to domestic and foreign franchisors:

> *Article 32(1) "catering chain" means a sizeable catering service business using a single brand name, implementing central and standardized management under a chain store corporate headquarters, with ten or more than ten outlets (including, direct stores, franchise stores and joint ventures etc.)*
>
> *Article 32(2) "chain store corporate headquarters" means operating entity implementing central and standardized management towards all catering chain outlets under a single brand name as authorized by such entity.*

Franchisors may be caught within this definition. However, Article 6 must be noted for an important qualification to this definition:

> *Article 6 The entity running a catering chain under a single brand shall clearly name a chain store corporate headquarters. The chain store corporate headquarters shall have the capability to manage a catering chain, and have secured governmental permission to conduct food business "catering chain service management", and bear the food safety management responsibility of branches[361], central kitchen and outlets.*

The prevailing view among lawyers in China is currently that foreign franchisors having no team in China shall not fall within the definition of "chain store corporate headquarters". A franchisor or a master franchisee / sub-franchisor in China who exercises a considerable degree of supervision and control over the operation of a local franchisee may fall within the scope of this definition, but it is open to interpretation what degree of control might be deemed sufficient to cross this threshold. If the franchisor or master franchisee is merely supervising the operations of the multi-unit franchisees or sub-franchisees and not exercising a sufficient degree of control, one may argue that the franchisor or master franchisee should not be considered as the chain store corporate headquarters under the Corporate Liability Regulations. On the contrary, if most of the franchisees or sub-franchisees are single-unit franchisees, and the franchisor or master franchisee is exerting significant control and enforcement power over the franchisee's compliance with standards, the outcome should be different. There has not been any interpretive guidance by any governmental authority to date, so an expansive scope of the language in Article 32 is advisable. Therefore, if there is a local team of franchisor or

[359] Articles 2, 26(2), and 26(4).
[360] Articles 9, 27.
[361] There is a definition of "branches" under Article 32.

master franchisee in China to support the franchisees or sub-franchisees, there is need to consider if such entity is exposing to the responsibilities and liabilities of chain store corporate headquarters under the Corporate Liability Regulations.

Once the franchisor or master franchisee is deemed to be the chain store corporate headquarters, there are system implementation, record keeping, regular audit, and reporting requirements imposed on them by the Corporate Liability Regulations[362].

Indeed, some local administrations have issued local detailed rules which inform the Corporate Liability Regulations. There are reporting requirements imposed on chain store corporate headquarters, and some the franchisors or master franchisees may be requested to report to the local authority as the corporate headquarters[363]. This requirement could arise for franchisors in one of two ways: (i) either a subsidiary of the franchisor is operating as the sub-franchisor, and has the same high degree of supervision as the franchisor, or (ii) a local team designated by the franchisor may be authorized to exercise a high degree of supervision.

4. Takeaways

To plan for the legal developments described above, franchisors would be well-advised to:

- review record keeping systems in light of the Outsourcing Rules and different local rules on pre-made dishes (if applicable);
- consider if there is need to have an on-site inspection team at the more important contractor's production locations;
- consider dual-suppliers modus, even if the central kitchen has been set up to avoid disruption of supply due to food safety incidents; and
- if there is a local team in China, there is need to check if such team is exposing the franchisor or its subsidiaries to the responsibilities and liabilities under the Corporate Liability Regulations.

D. PRE-PAID CARDS AND PRE-PAYMENT SCHEMES

Effective May 1, 2025, the Supreme People's Court issued a Judicial Interpretation[364] on the Application of Laws for Adjudication of Consumer Pre-payment

[362] Articles 7 to 23.

[363] See Article 9 of Wan Shi Jian Can Yin (2026) N0.1, *Anhui Province Catering Chains Food Safety System Inspection Administration Rules (Tentative)* (2026). Such Rules did not define what is corporate headquarters, but upon a quick exchange with an officer, franchisors and sub-franchisors may have to observe these requirements if they are taking the food safety supervision responsibility, particularly in cases of having considerable number of single-unit franchisees in Anhui.

[364] China is not a common law jurisdiction. A Judicial Interpretation of the Supreme People's Court is conceptually like a organized collection of rulings after considerable amount of actual decisions on the same subject matter.

Related Disputes[365] (the "Judicial Interpretation on Pre-payment Disputes"). An analysis of these provisions first requires a need to understand the background of the Judicial Interpretation on Pre-payment Disputes. Prior to the release of the interpretation, there were rules on the administrative recordal of consumer pre-paid cards (including virtual cards) and management of funds announced by the Ministry of Commerce366. However, the following issues in recent years have been of particular concern: (a) pre-payments by minors on online game platforms, and (b) chain stores (e.g. fitness centers, fast food outlets, beverage kiosks, and cafes) went bankrupt or moved to another location after receiving a considerable amount of pre-payments from customers. As the interpretation of existing law falls within the domain of the Supreme People's Court, the Judicial Interpretation on Pre-payment Disputes was released.

Of note, certain localities have already implemented further local rules on prepayment arrangements. In January 2026, the municipality of Shanghai issued new regulations on prepayments[367].

1. Franchisor's Liability under the Judicial Interpretation on Pre-payment Disputes

The Judicial Interpretation on Pre-payment Disputes address certain consumer protection matters of potential relevance to franchisors, including rules against unfair one-sided contractual terms, rules against unilateral change of conditions368, and a consumer's right to ask for refund in case of change of location.

Article 5 of the Judicial Interpretation on Pre-payment Disputes specifically addresses the liabilities of franchisors. In the event that a local franchisee enters into a pre-payment contract with consumers, the franchisor can be held liable if that franchisor agrees to be bound by such contract or admits its liability under such contract, or there are provisions in the contract authorizing the consumer to recover damages against the franchisor, though this is most likely to arise only where the franchisor enters into a contract with the consumer directly and receives payment from the consumer. Most often, these steps will be facilitated by the local franchisee, and it is likely only in exceptional circumstances that a franchisor deals with the consumer and would be exposed to this potential liability.

Under the same Article 5, in the event of the franchisor's action, inaction, omission, and/or negligence cause damages, and/or increase damages suffered on the part of the consumer, the Court can hold the franchisor shall be liable, as well. This provision places a heavy burden on the franchisor to supervise the franchisees in case such pre-payment cards and schemes exist.

---

[365] Fa Shi (2025) No.4.
[366] *Single purpose Commercial Pre-paid Cards Management Rules (Tentative)* (2012, amended in 2016).
[367] *Shanghai City Single Purpose Pre-paid Consumption Card Administration Regulations* (2026)
[368] Article 9.

2. Takeaways

With respect to prepaid charges which franchisees in China will accept, franchisors should:

- implement more detailed rules on pre-paid cards or pre-payment schemes and arrangements;
- consider if the franchisor should play a more active role in managing the funds; and
- regularly inspect and audit franchisees' operations to ensure these laws and regulations and internal rules are being followed.

E. SAFE HARBOUR RULES UNDER ANTI-MONOPOLY LAW

Historically, there has been considerable uncertainty with respect to whether vertical agreements on pricing and market partitioning in franchise systems with franchisees in China can be exempted under the safe harbour rules and the Anti-Monopoly Law. To date, the National Administration of Market Regulation has been hostile towards all manner of vertical agreements on pricing. The National Administration of Market Regulation issued the amended Anti-Monopoly Agreement Rules in December 2025 after a long consultation process, and the most relevant portion for franchisors with franchisees in China is that the scope of safe harbor has now been determined.

For vertical monopoly agreement regarding resale pricing and minimum pricing369, in the event the respective markets shares of all parties in a vertical monopoly agreement are lower than 5%, and the aggregate annual sales turnover of these parties for the subject products is all along less than ¥RMB 100 million (approximately $USD14.541 million370), such vertical monopoly agreement shall be exempted if such agreement does not impair competition within the market371.

For a vertical non-pricing monopoly agreement such as an agreement for geographical market partitioning, in the event the respective market shares of all parties of the agreement is less than 15%, such agreement shall be exempted if such agreement does not impair competition within the relevant market372.

The next step in the analysis, then, is what constitutes a relevant market. Although the Anti-Monopoly Committee of the State Council issued a guideline on market definition in 2009373 which provided for basic principles, there is a general lack of judicial precedent for franchisors and consumer products and services. The most relevant case for defining a market of food products came from an administrative determination on

---

369 See Article 18 of *Anti-Monopoly Law* (2022).
370 At exchange rate RMB 1 = USD 0.15 (March 12, 2026).
371 Article 17 of *Anti-Monopoly Agreement Rules* (2025).
372 *ditto*.
373 *Guidelines on Market Definition issued by the Anti-Monopoly Committee of the State Council* (2009)

merger control regarding the acquisition of SAB Miller by Anheuser-Busch InBev, in which beer should be separated from other alcoholic products due to (a) consumer behavior, and (b) the ingredients used, way of production, and alcoholic content; while ¥RMB 5/500ml was adopted as the line between beers for lower market and other beers for middle market374.

Since the Anti-Monopoly Agreement Rules have been recently released, it will take additional time to better understand more about the application of these safe harbor rules.

F. 2025 ANTI-UNFAIR COMPETITION LAW AMENDMENTS

The Anti-Unfair Competition Law was recently further amended after amendments made in 2019. The newly introduced parts which are more relevant to franchisors and franchise operations concern internet behaviour, consumer protection, and abuse of substantial market status.

Unauthorized use of other's name of application, domain name (or prominent part thereof), new media, website layout which is known by the public of considerable extent e.g. using part of a popular new application's name as internet keyword are now expressly prohibited375. Further, deceptive marketing tactics such as paying reviewers, fabricating order volume by false orders are also now prohibited nationally (previously, these prohibitions existed at certain administrative rules)376. Posting malicious negative comments towards competitors, and organizing joint actions to return goods after ordering from a competitor is also prohibited377.

Unilateral change of terms in a promotional contest once the contest has begun is also prohibited378. The ceiling of value of any prize remains at ¥RMB 50,000379.

Interestingly, the law also introduces the competition law concept of abuse of market position. In the event that a large entity abuses its market position to compel smaller players (e.g. smaller suppliers) to accept patently unreasonable conditions (such as an excessively long payment cycle, unreasonable payment delays, or liabilities for breach of contract that are disproportionate to the actual breach), the court can intervene380. Of relevance, however is that the phrase "market position" used here has

---

374 Announcement of Ministry of Commerce No. 38 (2016), *The decision of Anti-Monopoly Report in relation to the Acquisition of shares of SAB Miller by Anheuser-Busch InBev* (2016). The decision was very concise and the authority did not elaborate further on the basis of reaching such market definition. Of course, in recent years, new published decisions are with elaborated reasoning but we are still waiting for a case directly on market definition for food and catering sector.
375 Article 7(3).
376 Article 13.
377 Article 13.
378 Article 11(2).
379 Article 11(4).
380 Article 15.

a different meaning from the phrase “dominant market position”, which is adopted under the Anti-Monopoly Law. The former refers to the substantial imbalance in bargaining power between the parties within a specific transactional relationship, rather than their control over the relevant market as a whole.

G. NEW LAW ON COMMERCIAL MEDIATION

Commercial mediation is growingly common in disputes in China. Although there is a *de facto* practice of mediation in court litigation in China, mediations in China have been conducted without a clear legal status nor procedural standards. The Commercial Mediation Regulations, which will be effective from May 1, 2026, will fill this gap. The policy signal is clear: China intends to have commercial mediation professionalized and positioned as a reliable third option alongside with litigation and arbitration.

Commercial mediation is voluntary and confidential[381], and in the event of parties failing to reach any agreement, the mediation should be terminated[382]. Written mediation agreements should be produced upon reaching a settlement383. Since China is a party to the UN Convention on International Settlement Agreements Resulting from Mediation (Singapore Convention), mediation agreement is also enforceable outside China and vice versa384.

It is expected that certain national or regional mediation bodies will soon be established and consolidated, and more detailed rules will be released on the practice and procedures.

H. 2025 ARBITRATION LAW AMENDMENTS

On September 12, 2025, the State Council Standing Committee of the National People’s Congress enacted the revised Arbitration Law. This law became effective on March 1, 2026, and marks the most substantial effort to modernize the country’s arbitration law regime.

The new arbitration law maintains the existing framework that Chinese courts are the exclusive authority to grant interim or conservatory measures in support of arbitration. The amendments now expand the kinds of reliefs and parties can now seek injunctive and mandatory orders (in addition to property and evidence preservation) from the courts385. However, different from injunctive and mandatory orders in common law jurisdictions, these orders aim at preserving the status quo or avoiding irreparable damages to one party. In fact, the relevant rules on injunctive and mandatory orders under the Civil Procedure Law were introduced a few years ago. Available typical cases are relevant to intellectual property enforcement, and therefore whether such injunctive

[381] Articles 14 and 15 of *Commercial Mediation Regulations* (2025).
[382] Article 21.
[383] Article 22.
[384] Article 23.
[385] Article 39 of PRC Arbitration Law (2025).

and mandatory orders can cover non-intellectual property contractual issues remains a question to be answered.

The new arbitration law allows online arbitration[386]. A party seeking to set aside an arbitral award in China must apply to do so within three months of receipt[387], as opposed to six months under the previous law.

The previous law did not recognize the concept of the "seat", i.e., place of arbitration. Contrary to the widely accepted position in international arbitration, the seat of arbitration can be different from the physical location of the administering institution or the venue where hearings are held. The new law formally recognizes the concept of the arbitration seat in relation to foreign-related arbitrations[388], by providing that parties to a foreign-related arbitration may now agree on the seat of arbitration in writing. It further clarifies that an arbitral award is deemed to be made at the seat, and absent agreement to the contrary, the seat determines both the procedural law governing the arbitration and the court with supervisory jurisdiction.

For international franchise businesses in particular, if the ability to obtain swift injunctive relief is crucial to protect brand integrity, whether selecting an arbitral seat outside China should be carefully considered.

[386] Article 11.
[387] Article 72.
[388] Article 81.