Seyfarth

Commercial Litigation Outlook

2026 Edition

Table of Contents

Introduction

—By Shawn Wood and Rebecca Woods

The sixth edition of our Commercial Litigation Outlook arrives at a moment when change feels less like a trend and more like a standing condition.

Businesses, courts, and policymakers are confronting legal, economic, and technological pressures that are accelerating rather than stabilizing. From the widening reach of artificial intelligence to the steady march of state legislatures into areas once dominated by federal regulators, the themes highlighted here reflect a risk landscape that is dynamic, fragmented, and increasingly resistant to tidy predictions.

Artificial intelligence again takes center stage, and unlike earlier cycles of enthusiasm, its impact today is concrete enough to create real legal consequence. AI-enabled tools are reshaping internal operations and litigation strategy, even as they raise difficult questions about inadvertent disclosure, the authenticity of AI-generated content, and the risks associated with ever-more convincing digital forgeries. Courts have only started to wrestle with what it means to authenticate AI-created materials and the scope of discovery with respect to the use of those tools. At the same time, businesses are struggling to protect ownership rights in content that is neither entirely human nor entirely machine-made. With state and federal governance of AI shifting as quickly as the technology itself, organizations must adopt policies and guardrails that address their use of AI.

AI's influence expands well beyond discovery and intellectual property. Algorithmic pricing tools continue to attract the attention of antitrust and consumer protection regulators, and the availability of deepfake technology presents significant challenges to businesses. As AI moves from novelty to infrastructure, businesses must ensure that their use cases align with emerging legal standards. In short, the technology may be futuristic, but the compliance fundamentals are not.

Restrictive covenants are experiencing their own period of turbulence, driven largely by state-level activity. With federal efforts toward a nationwide non-compete ban stalled, several states, including Texas, Arkansas, and Maryland, have moved to narrow enforceability, particularly in heavily regulated sectors like health care. Others have taken the opposite approach, positioning themselves as safe harbors for employers. The result is a patchwork that demands careful, jurisdiction-specific calibration. Meanwhile, remote work and cloud-based collaboration continue to expose weaknesses in trade secret protections, underscoring the need for employers to strengthen their confidentiality and access protocols.

Privacy enforcement continues to gain momentum, with states stepping in to address growing concerns around data collection, biometric information, and transparency. California remains the bellwether with ongoing refinements to the California Consumer Privacy Act, prompting similar obligations across Texas, New York, and elsewhere. These developing frameworks introduce significant compliance burdens, even as courts impose higher bars for proving injury. Plaintiffs remain active, and state enforcement related to robocalls, hidden fees, and data security continues to expand. Biometric privacy, in particular, has become a major driver of litigation risk, and businesses must treat data governance as a trust and credibility issue rather than merely a technical one.

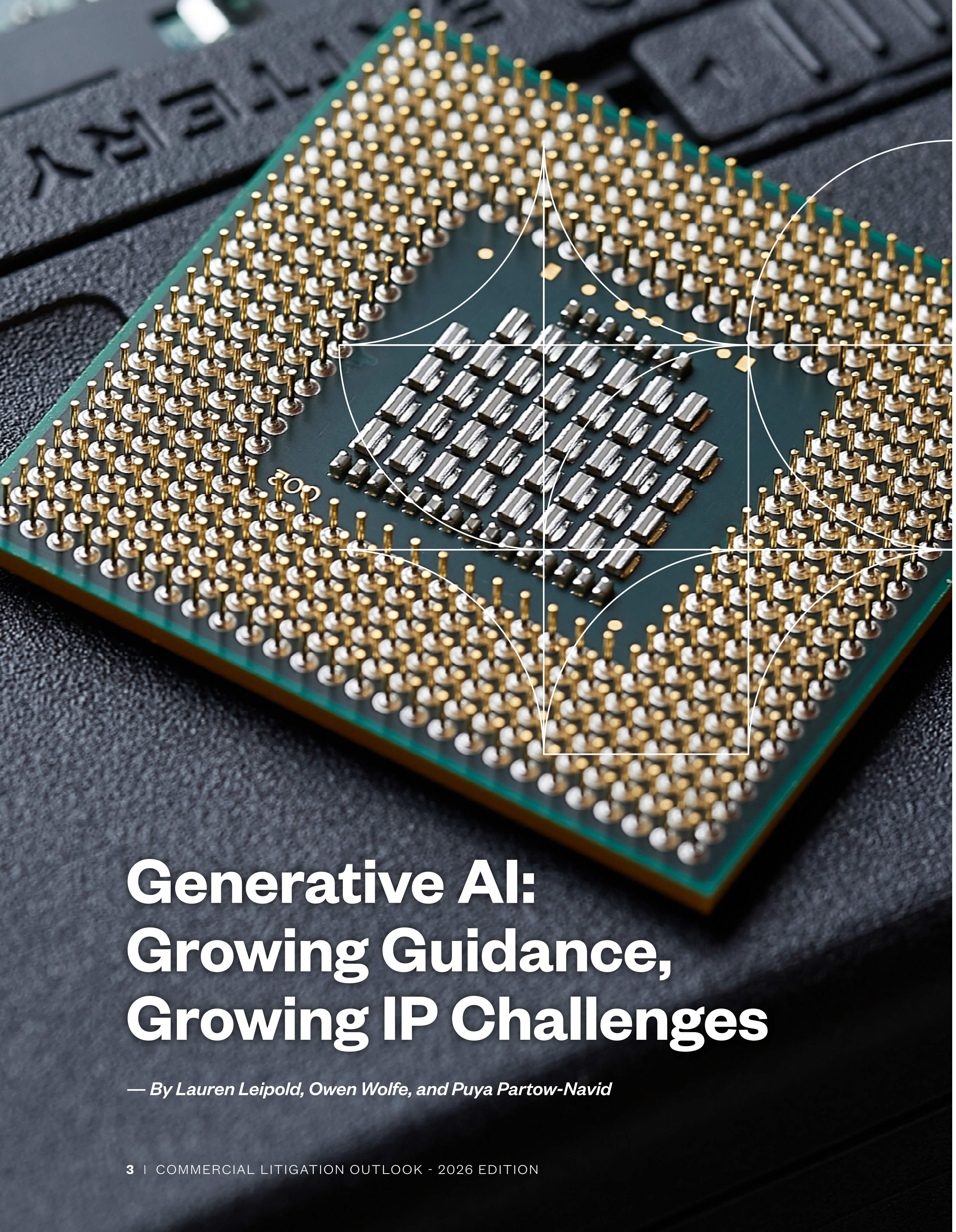
The False Claims Act remains a powerful tool in the government's enforcement arsenal, although recent Supreme Court decisions, including Schutte and Polansky, are reshaping important aspects of liability and case procedure. The Department of Justice's Whistleblower Pilot Program adds new incentives that will require close monitoring. For businesses operating in heavily regulated environments, the most effective protections continue to be contemporaneous documentation, calibrated compliance, and a culture that surfaces issues early.

Economic pressures are also shaping litigation trends. High interest rates, rising consumer debt, and the expiration of pandemic-era support programs are driving sustained financial strain across industries. Bankruptcy filings are expected to increase, particularly among franchisees and in commercial real estate and healthcare. In real estate, the gulf between top-performing assets and those constrained by interest rates, construction costs, and climate-related risks continues to widen, generating more disputes involving landlord-tenant issues, guaranty obligations, and foreclosures. Healthcare is experiencing similar stress points, driven by regulatory complexity and rising costs.

As we look ahead, one reality stands out: the commercial litigation environment remains fluid, fast-moving, and defined by competing pressures. Rapid technological advancement, shifting policy priorities, and evolving theories of liability will continue to test businesses and their legal teams. In the words of futurist Alan Kay, "the best way to predict the future is to invent it," a reminder that uncertainty, while often uncomfortable, also creates space for strategic reinvention. The forces described in this Outlook may complicate the year ahead, but they also present meaningful opportunities for adaptation, innovation, and competitive advantage.

We hope this year's Commercial Litigation Outlook provides meaningful insight and practical guidance as you navigate the complexities of 2026 and beyond. Staying informed and proactive continues to be the most effective strategy for engaging with an evolving legal and economic landscape.

Disclaimer: Because laws, regulations, and technologies continue to change quickly, certain information in this Outlook may become outdated. To stay current on developments affecting your business, we encourage you to follow Seyfarth's resources for timely updates and analysis.



Generative AI: Growing Guidance, Growing IP Challenges

— By Lauren Leipold, Owen Wolfe, and Puya Partow-Navid

In the 2024 edition of our forecast, we addressed IP issues and generative AI technology when guidance from government agencies, legislatures, and courts was limited.

Since then, litigation, government pronouncements, and other developments have somewhat clarified the scope of AI-related IP rights and liability. Many patent-related questions are now largely settled. But copyright- and trademark-related issues persist. While this year looks to be another active year for legal developments, we may not get more clarity due to the lack of federal regulation and differing decisions from the courts.

The Federal Government Is Taking a "Hands Off" Approach to AI Regulation

Over the past several years, US AI policy has shifted from regulation under President Biden to deregulation under President Trump.

President Biden's 2023 Executive Order called for AI guidance from the US Patent and Trademark Office ("USPTO") and the US Copyright Office. The USPTO provided guidelines on AI and patents in 2024, discussed below. The Copyright Office also launched a study and published findings in stages. President Trump revoked Biden's Executive Order in January 2025, directing agencies to roll back those rules.

While federal legislation has stalled, some states have passed AI-related legislation. California AB 2013, enacted in October 2024, imposes two requirements on AI developers. First, they must disclose information about the datasets used to train AI platforms. Second, they must share whether the datasets include any IP-protected data, with certain national security-, military- or aircraft-related carveouts. It is unclear whether other states will follow in California's path. In December 2025, President Trump issued an Executive Order that, among other things, restricts certain federal funding for states that have enacted "onerous" laws. That same Executive Order calls on federal officials to "prepare a legislative recommendation establishing a uniform Federal policy framework for AI that preempts State AI laws that conflict with the policy set forth in this order."

We expect to see fewer initiatives addressing use of copyright-protected materials as training data for generative AI. We also expect that open questions regarding copyright and trademark rights will be left largely to the courts. However, California's new law went into effect on January 1, 2026, requiring companies to comply with those disclosure requirements. This may result in changes on a larger scale.

The USPTO Provides Clarity on AI and Patents

In 2024, US patent professionals were trying to understand how AI fit within the patent law framework. Examiners issued inconsistent rejections regarding subject matter patent eligibility under 35 U.S.C. § 101 (aka "Section 101") for AI-related inventions, and the USPTO's much-anticipated guidance was still pending.

That uncertainty has begun to settle. The USPTO issued policy updates: one defining who qualifies as an inventor, and another clarifying what constitutes patent-eligible subject matter for AI inventions. The first policy update arrived in early 2024, when the USPTO released its long-awaited guidance on AI inventorship. The agency confirmed that AI systems cannot be inventors, but inventions developed with AI assistance can qualify for patent protection if a human made significant contributions. The guidance grounded inventorship in the so-called *Pannu* test, which requires each named inventor to have made a meaningful contribution to the invention's conception.

The USPTO's position is straightforward: humans own the inventive process, even when AI plays an essential role.

Inventors and companies must show how human input shaped the invention by defining the problem, selecting data, tuning a model's architecture, or interpreting results. Pressing a button on an AI model is not enough. The USPTO's position is straightforward: humans own the inventive process, even when AI plays an essential role.

The second major update came in mid-2025, when the USPTO issued new guidance for examiners on subject-matter eligibility under Section 101. Examiners must: (i) issue a rejection only when ineligibility is "more likely than not," (ii) avoid labeling machine-implemented operations as mental processes, and (iii) distinguish between claims that involve an abstract idea and those that actually recite one. This shift directs examiners to assess claims holistically rather than dissecting them element by element, recognizing that the value of AI inventions lies in the interplay of components, not in any single algorithmic step. While some examiners appear to have missed the memo, the trend is toward a more predictable and balanced standard.

Since taking office in 2025, Director John Squires has refocused the USPTO on novelty, non-obviousness, and enablement, calling AI a transformative tool. The Office has reversed several Patent Trial and Appeal Board ("PTAB") decisions that rejected AI-related inventions, signaling a shift from a defensive to an enabling approach. It is also piloting AI tools to modernize examination, aiming for greater speed, transparency, and consistency. Applicants likely can expect fewer borderline Section 101 rejections, deeper substantive analysis, and more enforceable AI patents.

AI-training patents remain hard to enforce because most training occurs privately and leaves little evidence of infringement. Applicants can reduce risk by claiming observable inference-side behavior and protecting training data, model weights, and tuning methods as trade secrets. Recent USPTO guidance clarifies which AI innovations may qualify for protection and how to present them. Companies should keep detailed records of dataset selection, model design, and result interpretation to support inventorship and ownership if challenged. While AI itself cannot be an inventor, it has become an indispensable partner in invention, and the patent system is beginning to reflect that reality.

Courts Continue to Grapple With AI-Related Copyright and Trademark Issues

There has been extensive litigation over AI and copyright since the launch of ChatGPT in late 2022. As with inventors in the patent context, under the current legal framework, authors of creative works must be human. Stephen Thaler, whose application for registration of an AI-generated visual work was refused—on the ground that it was not "authored" by a human despite Thaler entering prompts that guided the AI's output—has asked the US Supreme Court to review his case. In January, the Department of Justice urged the Court to refuse *certiorari*, arguing that the prohibition on protection for machine-generated works is well-settled law. If the Court takes the case, it will have to address the tension between this stance and the Trump Administration's pro-innovation agenda.

> Ironically, there are more instances of infringement to identify and address because the same technology makes it easier to commit that infringement.

Other cases grapple with two open questions regarding copyright liability for: (1) training AI on copyrighted works; and (2) AI output that is alleged to be substantially similar to a copyrighted work.

Liability for training hinges on "fair use," where courts analyze: (a) the purpose and character of the use; (b) the nature of the copyrighted work; (c) the amount and substantiality of the portion used in relation to the entire copyrighted work; and (d) the effect of the use upon the potential market for or value of the copyrighted work. In a 2025 ruling involving the AI startup Anthropic, a California federal court addressed "fair use" in the training context. Anthropic allegedly trained its AI program using a digital library containing copyrighted works from two different sources: (1) digital copies of copyrighted works that Anthropic legally purchased in hard copy and scanned; and (2) downloading millions of copyrighted books from pirate websites. The court held that using legally-purchased works was "fair use," but using copies from pirate sites was not. The ruling led to a blockbuster, $1.5 billion settlement. The court has expressed some hesitancy about approving the settlement, explaining that the amount may not be enough of a "blockbuster." Nonetheless, in all likelihood, it will approve the parties' proposed arrangement in 2026. Federal courts are not necessarily ruling in a consistent manner, however, because "fair use" rulings are fact-specific: a 2025 Delaware court held that "fair use" did **not** protect a company that created its own summaries of another's copyrighted works and then used those summaries to train an AI program. Other courts are likely to reach different conclusions in 2026, based on the facts before them.

We may see even more inconsistency when it comes to liability for AI outputs as courts continue to weigh in on that issue. In late 2025, a New York federal judge declined to dismiss claims against OpenAI based on AI output that allegedly infringed on the *Game of Thrones* novels. The court found that certain AI outputs were attempts to abridge copyrightable elements of the books or were otherwise substantially similar to the books. The ruling only permits the case to proceed; it remains to be seen whether the court will find OpenAI liable. We expect to see additional copyright rulings in 2026 in that case and others, but not necessarily with any discernable rules emerging given the variances in very fact-specific decisions to date.

Moreover, there is at least one California case alleging that AI-generated images led to trademark infringement. Though less common, we expect to see more guidance in 2026 emanating from disputes regarding AI and trademark infringement. Indeed, generative AI programs are becoming more adept at generating images, and more companies are using AI-generated images in advertising, which will likely result in additional AI-related trademark disputes in 2026.

Companies Will Increase Use of AI to Detect (or Enable) Infringement

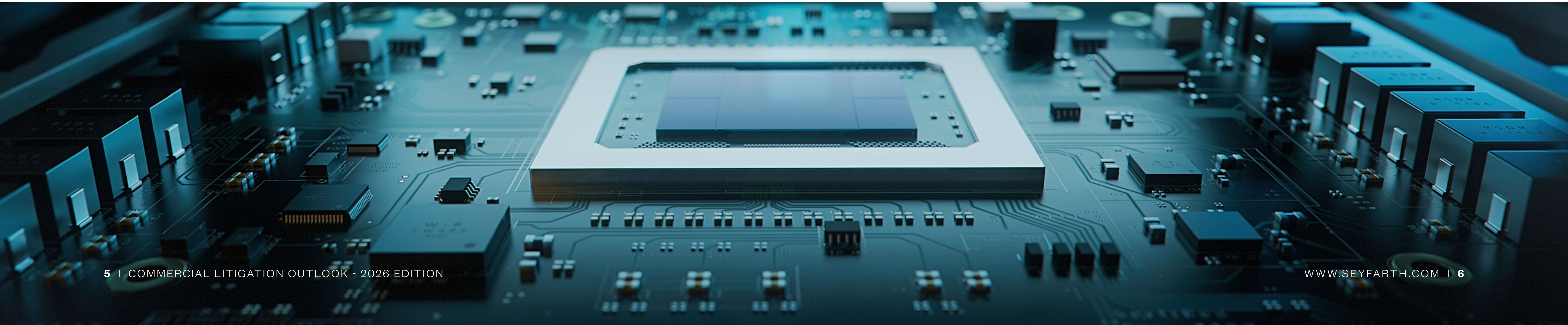
AI technology has assisted IP owners in identifying infringement more rapidly, using image recognition, text analysis, and pattern detection. It can be used in authenticating products to combat counterfeiting. AI helps to collect and analyze large swaths of customer data to create more effective marketing campaigns.

Ironically, there are more instances of infringement to identify and address because the same technology makes it easier to commit that infringement. Individuals with little technical skill can create infringing materials with the click of a mouse from anywhere in the world. Brand owners are reporting a significant increase in deepfake advertising materials that appear to be legitimate but might lead unsuspecting consumers to click on a phishing link.

There is no easy solution to these problems. Even if state or federal lawmakers regulate them, the practical difficulties of enforcement remain. We expect IP owners to continue to struggle to keep up, even with access to improved infringement-detection technology.

Conclusion

The legal landscape surrounding AI continues to change. In the absence of overarching federal laws, individual courts, states, and localities will continue to offer potentially competing views about how AI impacts IP rights. We expect companies and individuals to continue to integrate AI into their daily practices, for both good and nefarious purposes, undoubtedly leading to more litigation.



Key Trends in Commercial Litigation

Antitrust & Competition

— By Sam Rowley

A year ago, when the Trump Administration installed new antitrust leadership at the US Department of Justice (DOJ) and the Federal Trade Commission (FTC), the looming question was the extent to which the agencies would break from Biden era antitrust enforcement policies.

While the Trump Administration has restored a more traditional approach to some areas of antitrust law, the DOJ and FTC continue to pursue a muscular enforcement agenda.

Antitrust under the Trump Administration has in many ways adhered to the President's broader populist agenda. In December 2025, the White House directed the DOJ and FTC to investigate price fixing and anticompetitive practices in the food industry as part of an effort to address rising grocery bills. Earlier in the year, the FTC formed a Joint Labor Task Force to prioritize, among other things, anticompetitive labor-market practices that harm American workers, and upon assuming leadership of the DOJ's Antitrust Division, Assistant Attorney General Gail Slater emphasized publicly the role of antitrust law in protecting workers, not just consumers.

Above all else, the DOJ and FTC continue an intensive pursuit of Big Tech that began in the first Trump Administration. The agencies have pursued enforcement actions against nearly all of the leading Big Tech companies, with a particular focus on what they perceive to be illegal exercises of monopoly power under Section 2 of the Sherman Act. Big Tech should expect the DOJ and FTC to remain aggressive in platform-based enforcement, especially in the areas of search functions, advertisements, mobile device apps, and the cloud.

If 2025 is any indication, firms should also expect that artificial intelligence—and the uses to which it is put—will be a hotbed of antitrust enforcement in 2026 and beyond.

> Big Tech should expect the DOJ and FTC to remain aggressive in platform-based enforcement, especially in the areas of search functions, advertisements, mobile device apps, and the cloud.

AI: Algorithmic and Data-Based Enforcement

Thus far antitrust enforcement in the area of AI has centered on the use of algorithmic pricing tools. The core question is the extent to which competing firms may rely on non-public information shared through software programs to price products or services without violating antitrust laws. For example, the property management software provider RealPage has been defending its pricing tool on several fronts. The DOJ commenced an enforcement action against RealPage (as well as numerous multifamily apartment landlords) alleging that the use of RealPage's algorithmic pricing software facilitated illegal price coordination among competing multifamily landlords by sharing non-public data, leading to higher rents. RealPage argues that its software merely provides a lawful exchange of anonymized and aggregated pricing data for landlords to use in making their own independent decisions about the rents they charge. In November 2025, the DOJ announced a proposed settlement with RealPage that, if approved by the court, would require RealPage to, among other things, (i) not use real-time, nonpublic data of competitors in pricing algorithms; (ii) restrict its pricing model to historical information; and (iii) eliminate the collection of market-survey data. In announcing the settlement, Gail Slater emphasized that "competing companies must make independent pricing decisions, and with the rise of algorithmic and artificial intelligence tools, we will remain at the forefront of vigorous antitrust enforcement."

In a separate case brought against RealPage by private plaintiffs (multifamily tenants), in late 2025, a federal judge in Tennessee preliminarily approved settlements valued at $141.8 million that would resolve claims arising from the same theory pursued by DOJ—that the RealPage software facilitates collusion among landlords to inflate rents in US metropolitan markets.

The use of algorithmic pricing software has come under antitrust scrutiny in other industries. In August 2025, for example, the United States Court of Appeals for the Ninth Circuit affirmed dismissal of a complaint challenging the use of pricing software used by Las Vegas hotels. The Ninth Circuit concluded, among other things, that the independent, parallel adoption of the same pricing software provider by competing hotels was not enough to state an antitrust claim. However, consistent with its position in the RealPage case, DOJ filed an amicus brief in which it advocated for a robust stance against the use of centralized pricing algorithms. DOJ has also filed a statement of interest in litigation pending in the health insurance industry, similarly urging the court to adopt a broad application of the Sherman Act to the use by competing firms of algorithmic pricing software.

State legislatures are now taking action too. In December 2025, RealPage filed suit in federal court challenging New York's newly enacted prohibition on the use of AI pricing tools in rental markets as a First Amendment violation. Effective January 1, 2026, California banned the use or distribution of "common pricing algorithms" for anticompetitive purposes.

In short, recent litigation represents the first of an inevitable wave of antitrust scrutiny of the use of artificial intelligence. Firms will need to pay particular attention to the manner in which they use AI for pricing and data collection.

Merger Enforcement

While merger enforcement remains robust, the Trump Administration appears to also be receptive to business transactions. As a threshold matter, the DOJ and FTC elected not to rescind the 2023 Merger Guidelines adopted by the agencies under the Biden Administration. The 2023 Merger Guidelines, which identify the policies and practices the DOJ and FTC apply to investigate whether proposed mergers violate the antitrust laws, take a more interventionist approach than previous guidelines. The agencies also elected not to unwind the sweeping reforms enacted in 2024 to the Hart-Scott-Rodino Act (HSR Act), which governs the process by which parties must give the agencies an opportunity to review certain transactions for anti-competitive effects. The reforms substantially increased the breadth and depth of information that transacting parties must disclose to the agencies with their HSR notification and report filing.

> Firms will need to pay particular attention to the manner in which they use AI for pricing and data collection.

Despite upholding Biden-era reforms to the merger review process, 2025 showed that the Trump Administration is far more likely to resolve merger challenges consensually. This represents a stark departure from the DOJ and FTC under the Biden Administration, which did not shy from litigation intended to block transactions in their entirety. By contrast, the agencies in 2025 appear more willing to negotiate structural remedies to the transaction, which typically require that one or both parties divest certain business units or assets to resolve the anti-competitive concerns.

In announcing a settlement of one particular transaction, FTC Chairman Andrew Ferguson explained that structural remedies, rather than blocking deals outright, "may be the best way to protect competition" because "a settlement that successfully prevents the merger's anticompetitive features can strike a balance that permits the procompetitive aspects to proceed." He cautioned, however, that settlements should not "paper over an anticompetitive transaction." For transactions that present serious competitive concerns, the agencies therefore appear open to structural remedies that are robust enough to address the issues without the need for litigation.

Key Trends in Commercial Litigation

Bankruptcy Litigation and Restructuring

— By James Sowka

"It was the best of times, it was the worst of times...." Charles Dickens' century-old words aptly describe today's economic climate.

The contradictions in the US economy are likely to persist in 2026. Ultimately, the bankruptcy outlook will depend one's place in the "K-shaped" economy. Uncertainty around tariffs, inflation, and unemployment will remain defining features of the US economy, with many middle- and lower-end economic sectors facing distress, workouts, and bankruptcy.

The Tech and Jobs Sectors Reflect Today's Contradictions

The tech sector offers the clearest illustration of Dickens' words, but it certainly is not the only example. The AI tech boom is reshaping the US economy and workplace, creating the most valuable public companies in the world. The top five most valuable public companies by market capitalization in 2025 are all heavily invested in AI and have fueled a stock market boom resulting in a total market capitalization in excess of $16 trillion and now account for more than 50% of the value of the Nasdaq 100 Index. In 2019, those same companies had a market capitalization of less than $4 trillion.

> ...in 2025, employers across all industries announced layoffs exceeding 1.2 million—a feat that has only occurred 3 times in the past twenty years—during the global financial crisis in 2008 & 2009 and the pandemic in 2020.

Meanwhile, employers, including many adopting AI, accelerated announced job cuts in 2025. According to one survey, in 2025, employers across all industries announced layoffs exceeding 1.2 million—a feat that has only occurred 3 times in the past twenty years—during the global financial crisis in 2008 & 2009 and the pandemic in 2020. In contrast, employers announced 2025 planned hires of just 507,647, the lowest year-to-date total since 2010. Tech workers have been hit hard by job cuts in the past year with 154,445 announced job cuts. Across all industries, AI was cited as the express basis for 54,836 layoffs in 2025.

Commercial Real Estate Performance and Outcomes Will Continue to Diverge

First the good. The Federal Reserve Bank cut interest rates by a quarter point three times in the fourth quarter of 2025. These reductions are expected to stimulate deal flow in 2026, with private lenders expected to provide more than half of all commercial real estate loans. The AI revolution is also fueling a boom in data center construction with spending forecast to rise another 19.5% in 2026—following increases of 50% in 2024 and 33% in 2025. Class A office properties are expected to continue outperforming the broader office market. Similarly, luxury and upper-upscale hotels are expected to continue their strong performance into 2026, with higher occupancy rates and increased revenue and profits.

And the not-so-good. The outlook for additional Federal Reserve rate cuts in 2026 remains uncertain, clouding the overall outlook for the commercial real estate market.

> Delinquencies and workouts in commercial real estate will remain materially elevated in 2026 due to the so-called "Wall of Maturities" involving approximately $2 trillion in maturing commercial real estate mortgages through 2027.

Delinquencies and workouts in commercial real estate will remain materially elevated in 2026 due to the so-called "Wall of Maturities" involving approximately $2 trillion in maturing commercial real estate mortgages through 2027. While private lenders are expected to step in to meet the demand for refinancings, borrowers will face up to 50% higher costs for capital for maturing loans given that many of these loans were taken out prior to 2021 when rates were at near historic lows, which will strain profitability. Older Class B and Class C office buildings will face continued high vacancy rates and potential obsolescence requiring costly conversions to residential or other uses. Middle- and lower-tier hotels are projected to experience softer bookings and rising expenses that outpace revenue growth as consumers continue to wrestle with higher costs of living and labor market uncertainty.

Outside of the Luxury Sector, the Auto Industry Will Face Struggles from Affordability

Vehicle sales surged in 2025, but the outlook for 2026 is mixed. Luxury vehicles sales are expected to rise by 6%. However, affordability issues, rising car loan delinquencies, and bankruptcy filings by auto parts manufacturers and sub-prime auto lenders dim the forecast for the auto industry in 2026. Overall, it is predicted that there will be a 5% decrease in overall vehicle sales.

Affordability issues are at the forefront. The average price of a new car exceeded $50,000 for the first time in 2025, driven by tariffs, supply chain issues, and a larger number of luxury and electric vehicles sold. Tariffs, inflation, and uncertainty regarding further interest rate cuts in 2026 are expected to exacerbate overall affordability which will continue to strain consumers, especially subprime borrowers. Through the end of the third quarter 2025, 6.65% of subprime borrowers were more than 60 days late on vehicle loan payment—the highest level since 1994. More than 10.5 million vehicles are expected to be assigned for repossession in 2025 with more than 3 million vehicles predicted to be repossessed—nearing or potentially surpassing the record of 3.2 million repossessions set in 2009.

Bankruptcy Filings Will Again Increase in 2026 Fueled by Increases in Consumer Filings

As of September 2025, US courts reported a 10.6% increase in overall bankruptcy filings compared to 2024, marking the third consecutive year of double-digit growth. A closer look reveals increasing consumer distress: nonbusiness filings rose 10.8%, with Chapter 7 and 13 filings up 10.7%, while business bankruptcies increased only 5.6% and Chapter 11 case filings remained largely flat. Subprime auto repossessions are expected to drive further increases in consumer bankruptcy filings in 2026. While still at historically modest levels, chapter 12 farm bankruptcies increased a notable 45% in 2025, following a 42% increase in 2024. Farm distress is expected to increase in 2026 despite $12 billion in farm aid announced by the White House in the fourth quarter of 2025.

Conclusion

The "K-shaped" economy will continue to define the US economy in 2026, with the AI tech and certain other high-end sectors thriving, while other sectors, such as middle- and lower-market commercial real estate and the broader auto industry, grapple with significant challenges. Consumers will face continued affordability challenges as uncertainty from tariffs, inflation, and weak labor market persist.

Key Trends in Commercial Litigation

Consumer Class Actions

— *By Kristine Argentine, Joe Orzano, Aaron Belzer, and Paul Yovanic*

Consumer privacy-related claims—especially those involving broad collection and use of personal data—continue to dominate the class action space.

In 2026, courts, regulators, agencies, and legislators are expected to step up efforts to clarify or curtail several different statutes and regulations, including the California Invasion of Privacy Act and the Telephone Consumer Protection Act, that are driving these lawsuits. Such guidance will provide companies with much-needed clarity and leverage in defending these claims.

Telephone Consumer Protection Act (TCPA)

TCPA litigation has persisted for decades, but there was a significant uptick in 2025, which we expect to continue into 2026. This rise stems from businesses' increased use of text messaging and other technologies for mass marketing. A pivotal Supreme Court decision in *McLaughlin Chiropractic Associates, Inc. v. McKesson Corp.* (June 2025) will shape developments in 2026. This is because the Court held that the Hobbs Act does not prevent district courts from independently assessing agency interpretations of statutes, opening the door for courts to interpret TCPA provisions even when the Federal Communications Commission (FCC has issued prior orders and interpretations.

> By narrowing the permitted scope of arbitration, SB 82 increases the likelihood of consumer claims proceeding in court.

Already, cases in 2025 have invoked *McKesson* to seek independent interpretations on issues such as whether text messages qualify as "calls" and whether cell phones count as "residential lines" for Do Not Call violations. We expect many more positions taken by the FCC on the meaning of the TCPA—including enforcement of quiet hours—to be revisited in 2026.

Additionally, the FCC issued a Further Notice of Proposed Rulemaking (Oct. 29, 2025) seeking comment on whether to modify or abandon new rules related to the application of a consumer's decision to opt out of SMS messaging currently taking effect April 11, 2026. These rules would require businesses to apply a consumers opt-out request across all call types, not just the type of communication prompting the opt-out. The FCC is also considering changes to a 2025 rule prohibiting businesses from requiring a specific method by which a consumer can opt-out of receiving calls or SMS messages. By making these changes the FCC is looking to "modernize anti-robocall protections" and "eliminate outdated requirements that have been superseded by technology advances and calling practices." These evolving rules and interpretations will significantly reshape TCPA compliance in 2026.

California's Legal Shift: Arbitration and Privacy

California remains a focal point for consumer class actions, and major legal changes in 2026 will reshape the landscape.

Senate Bill 82 (SB 82), effective January 1, 2026, restricts overly broad arbitration provisions in consumer use agreements—contracts for goods, services, money, or credit. Historically, companies used expansive clauses to compel arbitration of disputes beyond the original transaction and limit class actions. SB 82 prohibits extending arbitration to unrelated future dealings or affiliated entities, rendering such provisions void and unenforceable. An agreement to waive these protections will be deemed against public policy.

This change has immediate implications: many arbitration and class-waiver provisions once enforced may now fail judicial scrutiny. By narrowing the permitted scope of arbitration, SB 82 increases the likelihood of consumer claims proceeding in court. Businesses relying on standardized contracts, online terms, or subscription agreements should review and revise dispute-resolution provisions now to preserve enforceability and mitigate litigation risk. In particular, companies should ensure that broad arbitration clauses expressly cover disputes "arising out of or relating" to the specific agreement, and that the underlying contracts include severability clauses to reduce the risk that an overbroad provision will be invalidated in its entirety.

Simultaneously, California's privacy framework is expanding. Updates to the California Consumer Privacy Act (CCPA) effective January 1, 2026, impose new obligations including:

- Confirming opt-out requests and streamlining "Do Not Sell or Share" processes.
- Ensuring mobile apps provide accessible privacy policy links.
- Requiring large social media platforms (over $100 million annual revenue) to offer clear account deletion mechanisms.
- Data brokers facing heightened transparency and operational obligations, including disclosure of data shared with foreign entities or AI developers and monitoring California's Delete Request and Opt-Out Platform (DROP).

The law also redefines "sensitive personal information" to include minors under 16 and mandates honoring authorized agent requests (opt-out, deletion, access). These changes increase compliance burdens and class action exposure.

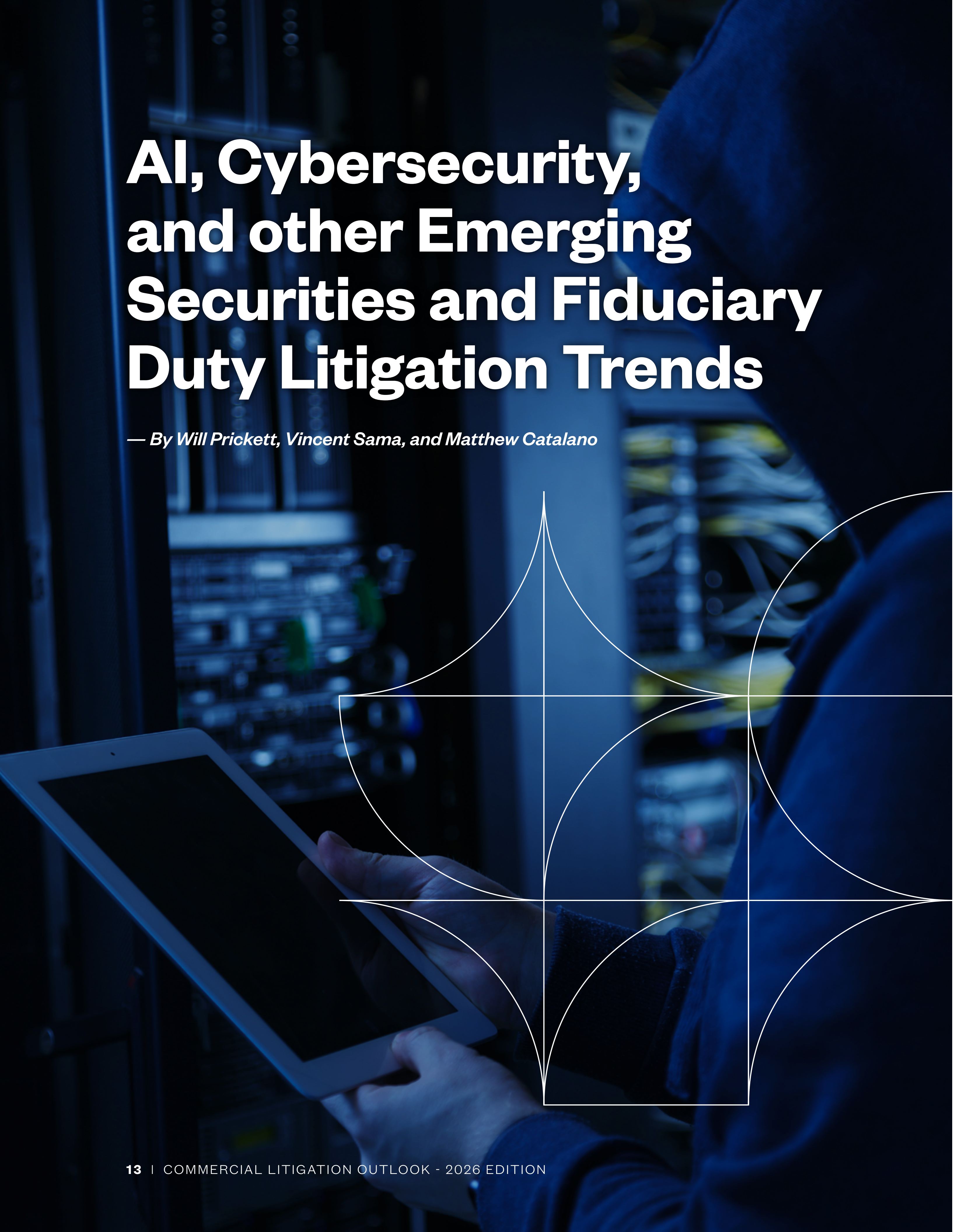
On the flip side, California is expected to amend the California Invasion of Privacy Act (CIPA) via Senate Bill 690, adding a "commercial business purpose exception." This exception would apply to permit use of certain online tracking technologies for legitimate business purposes and if they are otherwise compliant with privacy laws like CCPA. Though not retroactive, this exception will impact the future of CIPA litigation and provide an opportunity for defendants to make persuasive defenses.

Looking Ahead

Collectively, these developments signal a more complex and contentious consumer litigation environment in 2026 and beyond. Companies should act now to reassess their practices and reduce risk by:

- Tightening consumer contract language and disclosures.
- Modernizing compliance programs.
- Documenting processes thoroughly.

Looking ahead, businesses must also prepare for updated disclosure and transparency rules taking effect in 2027, governing automated decision-making technology (ADMT)—systems that substantially replace human judgment in making significant decisions about consumers, such as those involving credit, employment, housing, or education.



AI, Cybersecurity, and other Emerging Securities and Fiduciary Duty Litigation Trends

— By Will Prickett, Vincent Sama, and Matthew Catalano

Given advancements in AI, the ubiquity of data breach event-driven litigation, federal regulators' shifting priorities, and a business-friendly legislative change in Delaware, 2026 is likely to bring changes to the securities and fiduciary duty litigation landscape.

"AI Washing" and other AI-Related Investor Suits Expected to Rise

Much like now-familiar "greenwashing" allegations, the rapid rise in AI has led investor plaintiffs to allege that companies are making false or misleading statements about their AI usage, capabilities, or investments in what is being called "AI Washing." As companies continue to face market pressures to tout their adoption and implementation of AI technologies, they should take care to avoid statements that can be seized upon by investor plaintiffs to allege that AI usage is exaggerated, such as mischaracterizing non-AI technology (or human labor) as AI or overstating the potential business impact of the use of AI.

Furthermore, as AI-adoption becomes more widespread, securities suits premised on AI-related disclosures or activity are expected to rise, especially if publicly announced AI implementation plans do not pan out as expected. Investors may allege, for example, that a company did not adequately disclose the risk of replacing tried-and-true methods of operation and services with speculative or less proven AI technology.

Increased use of AI will also likely drive fiduciary duty claims in the coming year. A board or officer that over-delegates to an AI model may be accused of violating fiduciary duties, especially if the AI makes hallucinations or other mistakes that damage the business. Indeed, as companies race to adopt AI, insurance companies are rolling out "AI insurance" to supplement D&O and other policies that may not contemplate the unique litigation risks connected with AI.

Data Breach Securities Suits Are Expected to Continue Their Upward Trend

Over the past year, cybersecurity event-driven investor suits—claims that companies misrepresented or omitted cybersecurity risks leading to stock drop after a data breach, ransomware attack, or other cybersecurity incident—have continued to rise, with record-breaking settlements. This trend is expected to continue as data breaches become ever more ubiquitous and sophisticated, with the potential to wreak havoc on the company's stock price. Companies must of course maintain constant vigilance that their cybersecurity policies and procedures are up-to-date and followed. They should also take care with their public statements and risk disclosures surrounding data breaches and other cyber-attacks so they are prepared to address a securities suit in the unfortunate, but increasingly common, event that they fall victim to one.

In addition to traditional securities fraud suits, companies that fall victim to data breaches also expose themselves to derivative actions claiming breaches of fiduciary duty. A common theory asserted in such cases is the breach of a board's duty of oversight—a so-called "*Caremark* Claim." While *Caremark* claims were historically unsuccessful, in recent years they have seen a resurgence as the Delaware Chancery Court has permitted them to survive dismissal motions, especially where a board is alleged to have missed red flags leading to a failure of "mission critical" operations. Boards should consider implementing, and actively monitoring, a cybersecurity compliance system.

...the rapid rise in AI has led investor plaintiffs to allege that companies are making false or misleading statements about their AI usage, capabilities, or investments in what is being called "AI Washing."

SEC Enforcement Activity is Expected to Continue to Decline and to Reflect the Current Administration's Priorities

According to a Cornerstone report, SEC enforcement actions against public companies and subsidiaries dropped by 30% in fiscal-year 2025 (i.e. October 1, 2024 through September 30, 2025), 93% of which were initiated prior to the change in administration. Between voluntary departures, layoffs, and hiring freezes, the SEC saw significant staff reductions over the past year, and the current Administration's stated views on previous SEC priorities (such as ESG and cryptocurrency) suggest that there will be a further decline in overall SEC enforcement activity in 2026.

However, the SEC is likely to continue to pursue enforcement activity within the current Administration's priorities, including protecting national security and retail investors and combating alleged international fraud. For example, this past September, the SEC announced the formation of a "Cross-Border Task Force" which will focus on foreign-based companies, specifically identifying China as a jurisdiction "where governmental control and other factors pose unique investor risks." Companies should continue to employ strong Know Your Customer, Anti-Money Laundering, and Counter Terrorism Financing policies and practices, and should anticipate extra scrutiny from the SEC with respect to any foreign dealings, especially with China.

And while the SEC may be stepping back from what critics had called a "regulation by enforcement" model, the SEC is expected to continue to pursue activity in market manipulation, insider trading, and other traditional areas of enforcement against individual alleged bad actors. For example, in February 2025, the SEC replaced its sweeping Crypto Assets and Cyber Unit in favor of a smaller Cyber and Emerging Technologies Unit ("CETU"), signaling in the press release that CETU's focus would be to "root out those seeking to misuse innovation to harm investors and diminish confidence in new technologies" and otherwise to use SEC resources "judiciously" so as to "facilitate capital formation and market efficiency by clearing the way for innovation to grow"—messaging that indicates that traditional fraud would still continue to be pursued, even if in the AI, crypto, or other tech industry spaces.

Plaintiffs' Firms and Certain State Regulators Expected to Fill in the Enforcement Gap

Because prior SEC priorities under the Biden Administration, such as cryptocurrency and ESG, are no longer a priority for the Trump Administration, we expect a continuing reduction (though not a complete elimination) in SEC enforcement activity in these areas. However, that does not mean that Companies should take unnecessary risks. Plaintiffs' firms are expected to keep a sharp lookout for any plausible allegation that a company was emboldened to color outside the lines by a lax regulatory environment, and will continue to aggressively pursue greenwashing or crypto fraud claims. Furthermore, several states, especially those at ideological odds with the current administration, such as California and New York, are expected to respond to a reduction in federal agency enforcement by ramping up enforcement activity in their own jurisdictions.

Meanwhile, states and private litigants on the opposite end of the political spectrum are also anticipated to continue engaging in securities enforcement and litigation activity as a means to achieving their own political ends. For example, the "anti-ESG" movement remains popular, and we expect to continue to see litigants argue, for example, that the inclusion of ESG factors in an investment strategy breaches fiduciary duties. We also anticipate seeing a continuation of securities and fiduciary duty claims challenging companies' DEI policies, decisions to divest in certain industries, or other perceived left-leaning policies.

> the SEC is likely to continue to pursue enforcement activity within the current Administration's priorities, including protecting national security and retail investors and combating alleged international fraud.

Delaware's SB-21 Is Expected to Reduce Derivative Suits and Pretextual Books and Records Demands

Much commentary has been made of "DExit," which is the nickname for companies fleeing Delaware over the past two years for perceived "more business-friendly" climes of states such as Nevada, Wyoming, and Texas. Whether an actual phenomenon or exaggerated, in 2025 the Delaware legislature enacted SB-21 in an effort to nip DExit in the bud. This new law is designed to make Delaware even friendlier to corporations and their boards by, among other things, expanding the safe harbor for interested directors facing fiduciary duty claims and significantly curtailing books and records inspection requests. To the extent some companies had contemplated migration away from Delaware, SB 21 stands to reduce incentives for doing so by curtailing fiduciary duty derivative actions filed in Delaware and pretextual books and records requests (long a favorite of plaintiffs' firms seeking to circumvent the PSLRA discovery stay), or at least making responses to these requests more streamlined and manageable.

Potential for Mandatory Arbitration of Securities Claims

This past September, the SEC issued a policy statement reversing course on a "long-standing but unwritten SEC policy in which the agency blocked the Wall Street debuts of companies that want to ban shareholder class action lawsuits in their charters and bylaws." We anticipate that 2026 will see litigation as to whether such provisions are enforceable. Complicating such arguments for most companies, Delaware recently enacted SB 95, which plaintiffs are anticipated to argue prohibit mandatory arbitration due to its inclusion of the word "court" when discussing forum selection clauses.

In a recent speech, SEC Chairman Paul Atkins commented, that "[i]f SB 21 were one step forward by Delaware to modernize its Corporation Law, the prohibition of mandatory arbitration and fee shifting for federal securities law claims in SB 95 were two giant steps backward," but that "SB 95 was developed and became law at a time when the Commission had not made its views on mandatory arbitration clear to the public. With the benefit of clarity under the federal securities laws, I hope that the Delaware legislature will revisit the prohibition of both mandatory arbitration and fee shifting with respect to federal securities law claims." Should the Delaware legislature do so, and should mandatory arbitration clauses otherwise survive legal challenges, we could see a significant increase in mandatory arbitration of securities claims.

Conclusion

Given the rapid changes in technology and politics, we anticipate 2026 will bring unique challenges in securities and fiduciary duty litigation. Companies, directors, and officers should take stock of their AI and cybersecurity policies and procedures, understand how their company and its activities will be viewed by enforcement actors and plaintiffs on both the political left and the political right, and, for Delaware companies, update their books and records request response procedures to take full advantage of Delaware's recent legislative changes. Finally, they should keep an eye on litigation and legislative activity over mandatory arbitration of securities litigation.

Key Trends in Commercial Litigation

eDiscovery & Innovation

— By Jay Carle, Matthew Christoff, and Danny Riley

As we predicted last year, although generative AI ("GenAI") technologies have transitioned from experimental to practical within law firms and business organizations, it presents significant new discovery, evidentiary, and privilege risks.

In 2025, those risks were most visible in drafting tools, research assistants, and AI-enhanced review platforms where courts and litigants began testing transparency, validation, and work-product boundaries.

In 2026, that litigation pressure shifts to a new and pervasive category of tools: AI-enabled notetaking and meeting summarization. These tools are increasingly entrenched within virtual meetings as default features or automated (and infrequently disguised) "bot" participants. By recording a meeting, generating a transcript (often with speaker attribution), and automatically creating a summary of the meeting for potential distribution and retention, these tools transform routine meetings into new and unique discoverable records.

Looking ahead, inadvertent disclosure will remain the primary driver of risk to those utilizing AI meeting tools.

One of the greatest risks in the coming year is not simply that an AI-generated summary may be inaccurate, but that these tools may systematically convert live conversations into new and often unverified forms of evidence. In doing so, they (1) multiply the risk of inadvertent disclosure by capturing sensitive discussions that historically relied on discretion, (2) introduce evidentiary disputes when transcripts and summaries are later used to establish what was said, by whom, and how those discussions were interpreted or understood by the participants, and (3) create new avenues for legal claims against both developers and deployers of the technology.

Preventing Inadvertent Disclosure of Sensitive and Privileged Information

Without appropriate safeguards in place, AI notetaking tools can significantly increase the risk of inadvertent disclosure of confidential, sensitive, or privileged information. By their very design, these tools are constantly creating new documents, summarizing, aggregating, or attributing conversations that have historically been restricted to a targeted and predefined audience. Legal strategy discussions, internal investigations, and product or engineering reviews now routinely generate new, written records, often without any affirmative decision or approval by all participants to memorialize them. In the wake of numerous public incidents of employees uploading confidential information into public-facing large language models ("LLM") like ChatGPT or Copilot, organizations began to implement technical and educational safeguards to prevent the export of sensitive data outside the organization's control. It should come as no surprise that AI notetakers will require similar controls, particularly because, unlike LLMs, capturing a meeting can be automatically generated and the resulting output is specifically designed to be shared with others or retained for reference in the future. A single meeting can yield an audio file, a transcript with speaker attribution, and an AI-generated summary.

A common example that we predict will befall numerous organizations throughout 2026 is as follows: (1) a sensitive or privileged discussion is recorded with an AI notetaking tool "joining" the meeting; (2) an automated summary is generated along with speaker attributions; (3) a participant downloads the summary for review and validation; (4) the participant saves the revised summary in a discrete project folder or document management system; and (5) forwards a link or copy to the revised summary beyond the original meeting participants or fails to restrict access to the revised summary. Months later, that summary is subsequently collected and produced because it sits with the project's business records without a clear indication that it stemmed from a sensitive or privileged discussion.

Looking ahead, inadvertent disclosure will remain the primary driver of risk to those utilizing AI meeting tools. The organizations that fare best will be those that can document access restrictions, that sensitive outputs were segregated from general project repositories, and that the organization defined which record governs so automated summaries do not unknowingly become the operative account of events. Those same controls also set the foundation for defending the record when it is later offered as evidence.

Expect Evidentiary Fights Over AI Meeting Records to Rise

As AI-created transcripts and summaries become routine, they will increasingly be cited to support allegations or defenses, impeach testimony, reconstruct timelines, and argue who knew what and when. The resulting impact in litigation will be evidentiary disputes about authenticity, completeness, and context, particularly where multiple versions of these summaries exist.

In those disputes, the underlying facts surrounding the creation and handling of the transcripts and summaries may be unclear, particularly if they were created far in the past or if the original participants are no longer employed or available. Courts and adversaries will examine how recording and transcription were enabled, what settings governed the meeting recording and subsequent generation of the summary, where the authoritative copy resided, and how the documents moved across systems. These questions will often be difficult to answer when records are outdated, participants are unavailable, or summaries have been revised without documentation.

Reliability further complicates the evidentiary analysis. Meeting transcription is an imperfect process involving multiple speakers, overlapping voices, accents, organization-specific jargon or terms, and inconsistent or degraded audio, all of which are factors that increase the likelihood of errors that can only be resolved by the review of a participant within a reasonable timeframe after the meeting occurred. Automated summaries introduce an additional risk by paraphrasing rather than transcribing, and generative systems can omit emphasis or physical reactions such as surprise, a shaken head, or a thumbs up, they can overstate conclusions, or synthesize language that was never used. In litigation, those imperfections matter because small changes in wording or attribution can dramatically alter meaning, shift responsibility, or introduce uncertainty.

The practical consequence in 2026 is that the same control failures that drive inadvertent disclosure will also drive evidentiary disputes. When a party cannot show how meeting records were generated, validated, and controlled, there is a greater risk that transcripts and summaries will be challenged, as the same reliability concerns that allow a producing party to argue an AI summary should not be treated as a binding admission may also give the requesting party grounds to challenge its authenticity or completeness.

The Litigation Landscape Will Shift from AI Notetaking Tool Developers to Users

The risk posed by AI notetaking tools does not stop with inadvertent disclosure or evidentiary reliability. These tools also raise independent consent, privacy, wiretap, and biometric issues that are actively being litigated in court.

AI notetaking tools will reshape litigation risk in 2026 not because they are novel, but because they sit at the crossroads of discovery, evidence, and privacy law.

In *In re Otter.ai Privacy Litigation,* No. 5:25-cv-06911 (N.D. Cal. 2025), plaintiffs allege that Otter's AI notetaker automatically joined virtual meetings, recorded and transcribed conversations involving non-users without consent, transmitted meeting content to vendor servers in real time, retained recordings and transcripts, and used meeting data for secondary purposes such as model training. The consolidated action advances overlapping theories under federal wiretap laws, the California Invasion of Privacy Act, and the Illinois Biometric Information Privacy Act, demonstrating how a single meeting workflow can implicate multiple statutory regimes at once. That pattern is familiar. Early pixel-tracking and session-replay cases initially targeted organizations *developing* the tools before expanding to the organizations *deploying* the tools. We anticipate a similar trajectory here: in 2026, organizational users of AI notetaking tools will face increased scrutiny over implementation practices, including complications resulting from notetaking tools joining meetings by default and without announcement, how the distribution of summaries is controlled, and whether the organization can demonstrate how meeting data was captured, retained, and managed. Organizations with strong documented governance frameworks will be better positioned to defend against such claims. As with earlier waves of privacy litigation, liability exposure will increasingly hinge not on simply who built the tool, but on how it was implemented in day-to-day operations.

Conclusion

AI notetaking tools will reshape litigation risk in 2026 not because they are novel, but because they sit at the crossroads of discovery, evidence, and privacy law. What began as productivity and convenience amplifier now implicates consent, commercial surveillance, biometric, and wiretap laws while simultaneously generating records that parties must preserve, defend, and contextualize in litigation. As litigation trends shift from technology developers to organizational users, the key differentiator will be operational discipline. Organizations that treat AI meeting tools as governed systems rather than passive conveniences will be far better positioned to withstand the next wave of litigation scrutiny.

Key Trends in Commercial Litigation

False Claims Act, Whistleblower, and Qui Tam Lawsuits

— *By Chris Robertson and Teddie Arnold*

The False Claims Act (FCA) is poised for a significant shift in 2026 as diversity, equity, and inclusion (DEI) programs intersect with federal anti-discrimination mandates.

The starting point is the Bondi Memorandum (July 2025), which makes clear that recipients of federal funds cannot use race, sex, or proxies for protected characteristics in hiring, scholarships, or program eligibility—even under the banner of DEI. The memo's detailed examples—race-exclusive scholarships, "diverse slate" hiring requirements, proxy criteria such as "lived experience"—will serve as a blueprint for agency enforcement and private litigation. Contractors and grantees should expect these standards to influence audits, investigations, and FCA theories in the coming year.

Adding fuel to the fire is Executive Order 14173, which requires contractors and grant recipients to certify that compliance with federal anti-discrimination laws is *material to payment decisions* under the FCA. This language elevates DEI certifications from aspirational statements to high-risk representations. Under *Universal Health Services v. Escobar,* 579 U.S. 176 (2016) materiality hinges in part on whether the government would refuse payment if it knew of the noncompliance. With agencies now signaling that DEI compliance is central to payment, FCA exposure tied to DEI programs could expand dramatically.

Recent Supreme Court decisions continue to shape the risk calculus for DEI-related FCA exposure. In *United States ex rel. Schutte v. SuperValu Inc.,* 598 U.S. 739 (2023), the Court held that FCA scienter turns on a defendant's subjective belief, underscoring the importance of contemporaneous legal advice, internal deliberations, and documented compliance rationales as agencies scrutinize DEI-related representations. Procedurally, the Court's decision in *United States ex rel. Polansky v. Executive Health Resources, Inc.,* 599 U.S. 419 (2023) affirmed DOJ's broad authority to dismiss qui tam suits even after initially declining intervention, a tool DOJ may deploy if DEI-based theories begin to outpace its policy priorities. Adding another layer of uncertainty, a Florida district court in *Zafirov v. U.S. Department of Health & Human Services,* No. 8:22-cv-1835, 2024 WL 3011356 (M.D. Fla. June 17, 2024) held that the FCA's qui tam provisions violate the Appointments Clause. Although the ruling is on appeal and has no binding effect outside the case, defendants across numerous jurisdictions are already invoking *Zafirov* to challenge the structure of whistleblower-initiated FCA actions. Together, these developments signal that both the substantive and procedural contours of FCA enforcement may be unusually fluid heading into 2026.

What to expect in 2026:

- **Expanded FCA exposure** for DEI programs tied to federal funding, particularly in health care, higher education, and research.
- **Increased whistleblower activity**, pairing retaliation claims with FCA theories.
- **Agency scrutiny of third-party subawards**, as the Bondi Memo directs recipients to monitor downstream compliance.
- **Sustained enforcement pressure**, with DOJ reporting $2.9 billion in FCA recoveries for FY 2024 and signaling continued focus on fraud and false certifications.

Action items for contractors and grantees:

- Audit DEI initiatives against Bondi's risk taxonomy.
- Track and document agency knowledge to preserve materiality defenses.
- Replace demographic-driven criteria with job-related, neutral standards.
- Preserve contemporaneous records to meet *SuperValu's* scienter test.

> Executive Order 14173, which requires contractors and grant recipients to certify that compliance with federal anti-discrimination laws is material to payment decisions under the FCA. This language elevates DEI certifications from aspirational statements to high-risk representations.

Developments In Whistleblower Litigation

Whistleblower litigation is also poised for meaningful developments in 2026, driven by recent Supreme Court and appellate decisions that leave key issues—particularly causation and arbitration-related preclusion—unsettled.

THE STANDARD FOR CAUSATION UNDER SOX REMAINS UNSETTLED HEADING INTO 2026

It appears the applicable standard of proof in whistleblower matters will continue to be unsettled into 2026. Specifically, in the wake of the Supreme Court's decision in *Murray v. UBS Securities,* LLC, 601 U.S. 23 (2024) holding that an employee pursuing a Sarbanes-Oxley Act (SOX) retaliation claim need not prove retaliatory intent, the matter was remanded to the Second Circuit. Notwithstanding the Supreme Court's decision, the Second Circuit in February 2025 once again concluded that the jury verdict should be vacated, because the district court's jury instruction "strayed" too far from the text of SOX by expanding the definition of "contributing factor" beyond what the statute allows. The critical aspect of the jury instruction that the Second Circuit found problematic, which was not addressed by the Supreme Court, was the inclusion of language that allowed liability if the protected activity "tended to affect" the adverse employment decision, as opposed to actually influencing the decision. The Second Circuit's decision on this causation issue, which was not unanimous, is currently subject to a petition for review before the Supreme Court. Whether the Supreme Court will take this matter up yet again is unknown, but it does leave the issue of the proper standard for causation under SOX in limbo as we head into 2026.

ARBITRATION-BASED PRECLUSION CREATES NEW STRATEGIC CONSIDERATIONS

Also unsettled heading into 2026 is the law regarding the treatment of arbitrable and non-arbitrable whistleblower claims. In 2025, the Supreme Court declined to review the Ninth Circuit's decision in *Hansen v. Musk* (2024), which held that a confirmed arbitration Award denying a claim under Dodd-Frank collaterally estopped litigation in federal court of a parallel claim under SOX. Importantly, while SOX claims cannot be forced into arbitration, no such prohibition exists with respect to Dodd-Frank claims. The plaintiff argued that public policy prohibited applying arbitration findings to a federal statutory claim that is prohibited from being forced into arbitration. The Ninth Circuit majority, over a dissent, concluded that nothing in SOX prohibited the application of collateral estoppel, and noted that the plaintiff elected to pursue both arbitrable and non-arbitrable claims. Consequently, we expect in 2026 and forward that counsel representing plaintiffs in SOX cases will evaluate whether to bring multiple claims, and may limit the causes of action to avoid the prospect of a parallel arbitration that might have preclusive effect on non-arbitrable SOX claims.

What to Expect in 2026

- **Continued uncertainty** over the meaning of "contributing factor" under SOX pending possible Supreme Court intervention.
- **Expanded employer focus on documentation**, given heightened scrutiny of causation standards and the proof at trial that may be required.
- **More motions invoking collateral estoppel** where plaintiffs pursue both arbitrable and non arbitrable claims.
- **Increased strategic claim splitting** by plaintiffs seeking to avoid arbitration based preclusion.

Action Items for Employers

- Review and update whistleblower investigation protocols to ensure clear documentation regarding the issues raised and causation if there is adverse employment action.
- Train HR and compliance teams on the evolving causation framework under *Murray.*
- Preserve all contemporaneous decision making evidence to mitigate causation and preclusion risks.
- Re evaluate litigation strategy where employees assert both arbitrable and SOX based claims.

Franchise & Distribution

— John Skelton and Sam Rowley

Fierce competition, rising labor and food costs, increasing rents, reduced foot traffic, and, more recently, tariffs and inflation, have led to franchisee financial distress and bankruptcy filings, especially in the fast food industry.

In 2024 and 2025, there were several large franchisee groups that filed for bankruptcy. Franchisors should expect more franchisee bankruptcies in 2026. Because franchisee bankruptcies create serious issues, including negative publicity, dissatisfied customers, limited or shuttered operations, and litigation, franchisors need a comprehensive business strategy. The following are five essential elements of a franchisee bankruptcy strategy that plan franchisors should adopt.

1. Immediate Action. There is no "business as usual" for franchisors when a franchisee files for bankruptcy. For example, the automatic stay under 11 U.S.C. § 362 gives the debtor time to structure a reorganization plan by stopping (at least temporarily) collection and brand enforcement actions by the franchisor. The rules also allow franchisees to (i) continue to operate even if not fully compliant with a governing franchise agreement; (ii) sell its franchise at auction over the franchisor's objection; and (iii) prohibit a franchisor from issuing even routine notices of default absent stay relief. Because there are special rules governing financial transactions, franchisors should stop any electronic funds transfer ("EFT") procedures absent specific authorization. Franchisors also need to be ready to take immediate action to avoid waiver or loss of rights in the event of: (i) a debtor's request to use cash collateral to support its post-petition operations; (ii) a motion to assume executory contracts (i.e., the franchise agreement); (iii) selling the franchise; and (iv) conversion of the case to Chapter 7.

2. Engage with the Debtor. While the automatic stay prohibits any actions to collect pre-bankruptcy debt, franchisors need to engage with the debtor on its post-bankruptcy operations. Field personnel should continue to assess a franchisee's operations and document deficiencies in the ordinary course of the debtor's post-bankruptcy business (as long as they stay clear of any conduct that could be construed as an attempt to collect pre-bankruptcy debt in violation of the automatic stay). Engagement with debtor's counsel also often provides insight into the debtor's plans both as it operates during its bankruptcy and as it contemplates its exit from bankruptcy, and it allows the franchisor to address operational issues and weigh in with the franchisor's positions on any sale or other substantial transaction in the works during the course of the bankruptcy.

To terminate after the franchisee has filed for bankruptcy, however, the franchisor must show both good cause to terminate and for obtaining relief from the automatic stay.

3. Decide Whether Franchisee is Viable. Assessing viability is important because, unless the franchisee's plan is to liquidate, it will either seek to reorganize or sell itself as a going concern. If the franchisee cannot operate profitably post-bankruptcy (with the benefit of the automatic stay, debtor in possession financing, etc.), that likely means a successful reorganization is not likely to occur. To terminate after the franchisee has filed for bankruptcy, however, the franchisor must show both good cause to terminate and for obtaining relief from the automatic stay (i.e. the debtor is not meeting its post-bankruptcy obligations under the franchise agreement or the pendency of the bankruptcy case is otherwise causing harm to the franchisor). The mere fact the franchisee has filed bankruptcy is not enough. *See* 11 U.S.C. § 365(e)(1). The Bankruptcy Code contemplates that the debtor will need time to determine whether it will assume or reject the franchise agreement while it attempts to reorganize. *See* 11 U.S.C. § 365(d)(2) (generally allowing the debtor to assume or reject executory contracts at any time before plan confirmation). But that does not mean a franchisee can ignore its operational and performance obligations. *See, e.g., In re Lee W. Enterprises, Inc.,* 179 B.R. 204 (Bankr. C.D. Cal. 1995). Evaluating and documenting post-petition operations is critical because, without viable post-petition operations and adherence to post-bankruptcy obligations, termination may be justified.

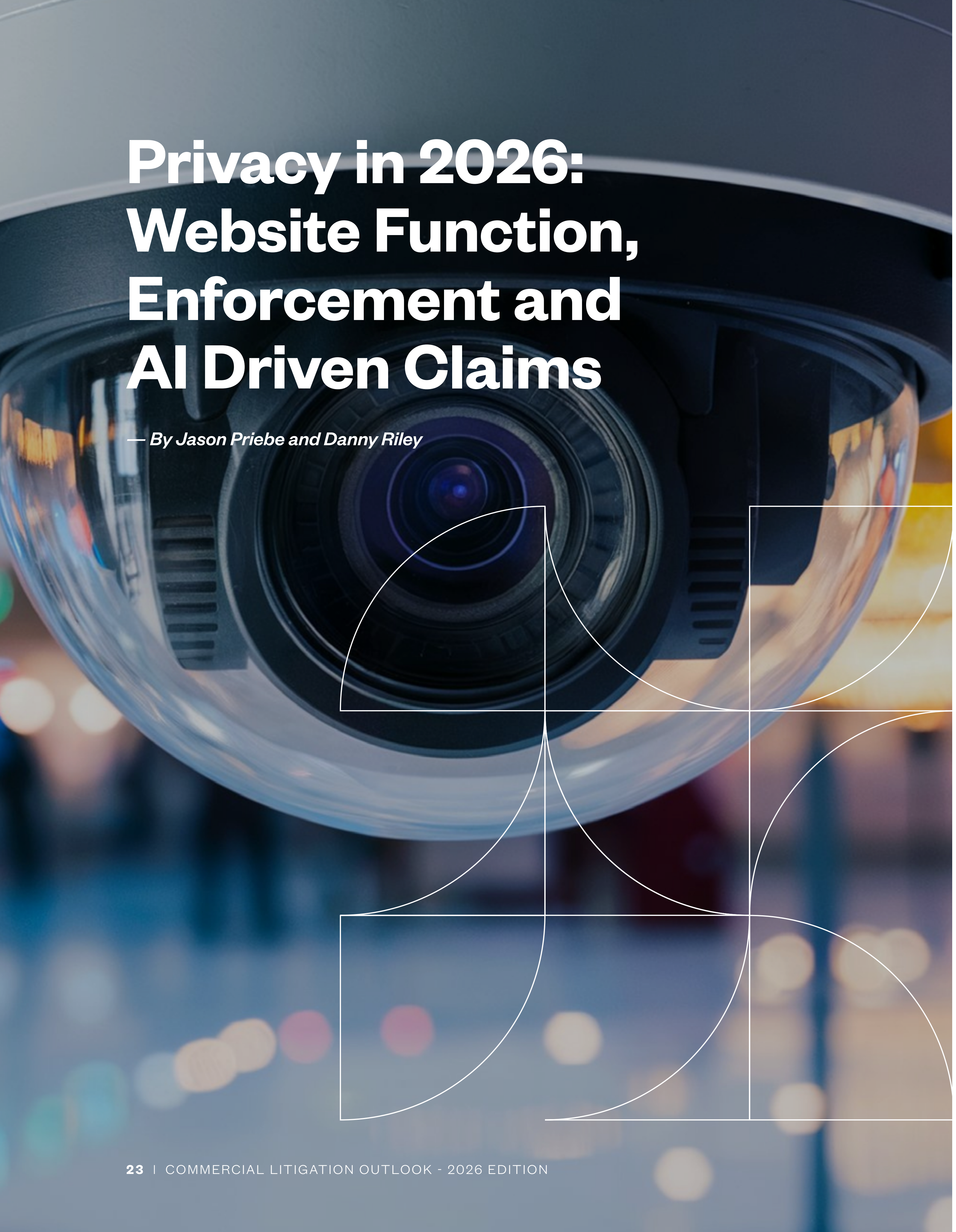
Once there is a bankruptcy filing, franchisors need to expect and prepare for litigation.

4. Protect Your Rights When There is a Proposed Reorganization or Sale. Besides liquidation, a bankrupt franchisee essentially has two options: (i) reorganize and seek to stay in business; or (ii) sell the franchise as a going concern. If there is a proposed reorganization, the franchisor needs to analyze the proposed plan carefully, especially to see if the plan seeks to modify any of the franchisee's obligations under its franchise agreement. As an executory contract, any proposed reorganization requires the franchisee to "assume" the franchise agreement pursuant to § 365. That means a franchisee must (i) cure any existing defaults (or provide adequate assurance of a prompt cure); (ii) pay any pecuniary losses suffered by the franchisor; and (iii) provide adequate assurance that the franchisee (or a proposed assignee) will be able to perform in the future.

A proposed sale presents other significant issues, including a proposed sale to a less-than-desirable buyer and an auction-type proceeding. Expect that all other constituencies will support the proposed sale, regardless of the buyer's qualifications or the impact on the franchise network. The franchisor must be proactive, especially enforcing its right to assess any proposed buyer, a decision which should not be subject to *de novo* review by the bankruptcy court. *See, e.g., In re Van Ness Auto Plaza, Inc.,* 120 B.R. 545, 546 (Bankr. N.D. Cal. 1990). Of course, consent should be contingent upon the debtor curing all material defaults and the buyer assuming all obligations under the franchise agreement.

5. Prepare for Litigation. A franchisee bankruptcy often means substantial losses for owners, investors, and creditors. Franchisees invariably blame the franchisor. The individual owners facing personal guaranty liability often have little choice but to sue or assert counterclaims in response to guaranty enforcement. Once there is a filing, franchisors need to expect and prepare for litigation.

There are, of course, other issues and considerations that can arise with distressed franchisees and dealerships. Some can be more straightforward while others involve complex financial, operational and network-related issues. Having a comprehensive business strategy can help navigate those issues. Among other things, working proactively with underperforming franchisees and dealers to help them avoid bankruptcy or mitigate the impact of bankruptcy is an important strategy. And if termination of the franchisee appears to be the best course of action, franchisors should consider initiating termination proceedings before the franchisee files for bankruptcy.



Privacy in 2026: Website Function, Enforcement and AI Driven Claims

— By Jason Priebe and Danny Riley

In our 2024 Outlook, we cautioned that tracking technologies and biometric claims were moving from commentary into courtrooms. In 2025, we predicted that generative AI and multistate coordination would reshape enforcement.

Both trends have converged: regulators and consumer litigants are now looking for website and application opt outs that really work for users, disclosures that mirror technical behavior, and disciplined handling of sensitive data. As we enter 2026, the focus shifts to whether companies can demonstrate, with live evidence, that their policy equals practice.

As we move into 2026, companies should prioritize periodic, evidence-based testing of opt-out mechanisms, cookie and pixel behavior, and vendor integrations in live environments. Maintaining documentation that ties disclosures to actual technical configurations, including data-flow maps and opt-out logs, will be critical as disputes turn on proof rather than intent. Organizations should steel themselves against even higher anticipated volumes of individual claims by aligning their internal privacy, product and engineering, and compliance teams around repeatable testing and remediation workflows.

As we move into 2026, companies should prioritize periodic, evidence-based testing of opt-out mechanisms, cookie and pixel behavior, and vendor integrations in live environments.

Enforcement has rewired expectations: privacy rights must be actionable, and disclosures must be technically accurate. In 2026, litigation will test those basics at full speed, amplified by AI driven request and complaint volume. The durable advantage isn't a clever argument. It is repeatable website and app testing and documented controls that turn policy into process. Companies that can show that type of proof will keep disputes narrow and stakes contained; those that can't will find that every banner, opt out click and every firing of a website beacon or pixel is now a potential claim.

Regulatory Enforcement Sets the Floor

The past year built a firm baseline for enforcement expectations, clarifying what regulators now view as table-stakes for privacy compliance. Across state and federal actions in 2025, regulators consistently focused on whether privacy rights worked in practice, not whether they were disclosed on paper (or more likely, “on screen”).

For example, to close the year, the California Attorney General entered a seven figure settlement with a mobile gaming publisher, for violations of the California Consumer Privacy Act (“CCPA”), including missing in-app opt-out mechanisms and the sale of minors' data. In parallel, the California Privacy Protection Agency imposed multiple fines and initiated its first public enforcement actions - including several six- and seven-figure settlements - faulting broken opt out flows, excessive verification, and nonfunctional cookie banners.

Outside of California, regulators demonstrated that privacy enforcement carries substantial financial consequences across a wide range of data categories. At the federal level, the Federal Trade Commission closed the year with a $10 million settlement with a major entertainment company for alleged violations of the Children's Online Privacy Protection Act, and a separate settlement of $500,000 with a large toy manufacturer after alleging the company's mobile companion app enabled the collection of precise geolocation data of minors by a third party without parental consent. At the state level, Texas secured a more than **$1 billion** settlement with a leading technology company in litigation tied to consumer data practices.

The recent enforcement trends span consumer-facing websites, advertising technology, geolocation data, connected tools and vehicles, and the collection of children's data. They all reflect a clear signal from regulators: privacy rights must function in practice, especially where sensitive data is at issue. Regulators are testing whether opt-outs *actually* work for consumers, whether consent mechanisms actually provide consumers with meaningful control over their privacy rights (and those of their children), and whether written disclosures accurately mirror a business' technical reality. Those same threshold issues are the factual backbone of modern privacy litigation.

Privacy in the Courtroom

Private litigation is increasingly tracking the same operational failures that drive regulatory enforcement. Rather than advancing novel privacy theories, plaintiffs are typically relying on older statutes and common-law claims to test whether modern consumer privacy controls actually function in practice. Across these cases, the alleged misconduct matches recent enforcement priorities: opt-out rights are “provided” in disclosures but fail technically; tracking and data collection occurs before a user has a meaningful opportunity to consent; or disclosures that understate how data is collected and shared.

Recent litigation under the California Invasion of Privacy Act ("CIPA") illustrates this convergence. In *Frasco v. Flo Health, Inc.,* No. 3:21-cv-00757-JD (N.D. Cal. 2025) plaintiffs alleged that software development kits embedded in a mobile health app intercepted user communications in real time and transmitted sensitive data to third parties, despite privacy disclosures assuring users that their data would not be shared. The case turned on whether technical data flows aligned with consumer-facing representations and whether users had meaningful control over sensitive information. After a jury returned a plaintiff-favorable verdict on the CIPA claim against one major tech company and other defendants resolved claims before trial, the matter ultimately concluded through a global settlement, with Flo Health, Google, and Flurry agreeing to pay nearly $60 million.

Traditional privacy claims present similar risks. In *Rodriguez v. Google LLC,* a federal jury awarded $425 million after finding that Google continued collecting data even after users disabled a privacy control intended to stop such tracking. (No. 3:20-cv-04688 (N.D. Cal. Sept. 2025)). The plaintiffs alleged that Google's "Web & App Activity" setting conveyed the promise of user choice, while back-end integrations continued collecting data from third-party applications, including ride-sharing, payment, and social media apps, without meaningful consumer control. The court denied Google's motion for summary judgment in January 2025, allowing the case to proceed to trial where the jury found Google liable for invasion of privacy under California's Constitution and for common-law intrusion upon seclusion. Although Google has announced its intent to appeal, the verdict underscores the exposure that can result when a privacy control does not operate as users reasonably expect.

AI tools now automate detection, evidence capture, and complaint drafting, reducing the time from failure to filing (or the receipt of a demand letter) to hours.

Taken together, these cases indicate to us that private litigation is not inventing new theories so much as enforcing, through damages actions, the same baseline expectations that regulators have set. Where pixels fire before consent, continue firing after opt-out, or operate differently than disclosed, those technical failures can trigger both regulatory scrutiny and private claims. In 2026, as AI tools make it easier to identify, document, and mass-assert these failures, the volume of pixel and similar CIPA-related disputes is poised to grow.

AI Is a Volume Engine

The same compliance gaps now driving regulatory actions and private litigation are also becoming easier to identify and assert at scale. What we expect to change in 2026 is not the legal privacy theories, but the ease with which individuals can surface, document, and pursue privacy complaints.

AI-enabled consumer tools increasingly automate privacy requests, track whether opt-outs are honored, and flag continued tracking despite user selections. Services such as PrivacyHawk, DeleteMe, and similar platforms allow users to submit opt-out requests across multiple services, monitor responses, and identify inconsistencies when tracking persists. Browser-based tools further assist savvy website users with the identification of issues by capturing cookie behavior and pixel activity that show whether data collection occurred before consent or continued after an opt-out. Once those failures are visible, generative AI lowers the barrier to escalation by assisting users with drafting. Soon, evidence of a nonfunctional opt-out or misleading control can be quickly converted into standardized complaints and demands, or *pro se* filings.

This pattern closely resembles what has recently occurred in website-accessibility litigation under the Americans with Disabilities Act ("ADA"). Under Title III of the ADA, businesses must ensure that websites function accessibly for users with disabilities. Over time, a repeatable model emerged where plaintiffs and "testers" verify compliance through objective technical checks, document failures with screenshots or code scans, and file high-volume, template-driven complaints asserting that the site did not work as required, regardless of intent or written policy. The plaintiffs' bar and opportunistic *pro se* litigants are now adopting the same playbook in privacy litigation. AI tools now automate detection, evidence capture, and complaint drafting, reducing the time from failure to filing (or the receipt of a demand letter) to hours. That acceleration means even minor implementation gaps can create exposure.

2026 Outlook

Privacy risk in 2026 will turn less on stated purpose and more on execution. Courts and regulators are converging on two practical questions: When is the consumer told they have a choice, and does the technology actually stop or allow data collection as promised? Increasingly, the issue is finally determined by how systems behave during real user interactions—not by policy language or design descriptions.

AI is accelerating this shift by shortening the path from technical failure to legal action. Tools that reveal tracking behavior, record user choices, and assist with drafting complaints make it easier for individuals to document problems and pursue them quickly. What once required sustained investigation can now follow directly from a single failed opt-out or misleading policy language.

The result is a litigation environment where small gaps can generate repeated disputes across regulators, courts, and arbitration forums. Companies that treat privacy controls as operational requirements—tested, monitored, and supported by clear records—will be better positioned to resolve issues early and limit exposure.

Health Care Litigation

— *By Jesse Coleman and Yumna Khan*

In the wake of a Texas federal court setting aside the Federal Trade Commission's (FTC) final rule banning most non-competes (and the FTC abandoning its appeal), states have responded with a wave of legislation in 2025 limiting the use of non-competes—particularly in the health care sector.

For example, Arkansas, Wyoming, and Maryland enacted laws voiding physician non-competes. Meanwhile, Texas limited the enforceability of non-competes for physicians to those terminated for cause, imposed buyout caps tied to one year's compensation, and imposed strict limits on geographic and temporal scope. In 2026, state legislative activity limiting non-competes is expected to continue.

Still, the FTC has not abandoned the issue. Instead, it is shifting to targeted enforcement (particularly in health care) through joint task forces, public inquiries, and case-by-case scrutiny. Recent actions include enforcement against a pet cremation company for imposing broad non-competes on nearly all employees and warning letters to major health care employers urging revisions to overly restrictive employment agreements. As broad regulatory efforts recede, 2026 is poised to become a year of focused crackdowns on non-competes at both the state and federal level. For more information, Seyfarth's "7 Areas To Watch As FTC Ends Push For A Noncompete Ban" offers further analysis and outlines practical ways employers can supplement their existing non-competes.

The New Era of AI Oversight in Health Care

2025 marked a turning point for AI regulation in health care. Forty-seven states introduced more than 250 AI-related bills, and 21 states enacted 33 of them. The surge reflects growing concern over AI's rapid integration in health care settings. The legislation falls into four main categories: (1) ensuring transparency in AI use; (2) protecting consumers by establishing rules on discrimination, disclosure, and decision making in AI; (3) establishing oversight for payors using AI; and (4) regulating how clinicians integrate AI.

Notably, six states—California (SB 243), Utah (HB 452), New York (SB 3008), Nevada (AB 406), Texas (HB 149), and Maine (HP 1154)—passed laws restricting the use of AI-enabled chatbots. This was largely driven by health care entities rapidly integrating AI chatbots to improve outcomes in clinical and administrative settings as well as concerns by legislators that AI chatbots may misrepresent themselves as humans, produce harmful or inaccurate responses, or not reliably detect crises. Five states—Texas (SB 1188), Nevada (AB 406), Oregon (HB 2748), Illinois (HB 1806), and California (AB 489)—also enacted laws restricting the use of AI in clinical settings. These include prohibitions in therapy settings, disclosure requirements when AI is involved in care, or bans on developers implying their AI systems can practice medicine. Finally, four states—Arizona (HB 2175), Maryland (HB 820), Nebraska (LB 77), and Texas (SB 815)—barred payors from relying solely on AI datasets or algorithms in decision-making. With many of these laws going into effect in 2026—and many more that will likely ensue in the 2026 legislative session—health care entities should anticipate stricter oversight and regulation into their use of AI in clinical and administrative settings.

Health Care Data Breaches and Data Privacy Litigation on the Rise

In 2025, health care data breaches dominated the privacy and data security landscape, with more than 500 large-scale incidents reported to the US Department of Health and Human Services Office for Civil Rights (OCR). The number of individuals affected from these large-scale incidents ranged from nearly 2 million to 10 million individuals. HIPAA enforcement also held steady. This was largely driven by the OCR's new enforcement initiative, which speeds investigations by focusing on the HIPAA Security Rule's risk-analysis provision—the most common violation. The surge in data breaches also fueled a sharp rise in data-privacy litigation, now one of the fastest-growing areas of US class actions.

Looking ahead to 2026, data breach risks will likely intensify as health care entities expand their use of AI and digital platforms to process vast amounts of personal, health, and biometric data. AI-based data processing also raises concerns of potential violations of data privacy laws, such as whether health care entities have proper consent from consumers to process sensitive data through AI. In short, these trends point to 2026 as a pivotal year for health care privacy, data security, and compliance.

False Claims Act ("FCA") Enforcement Shows No Signs of Slowing

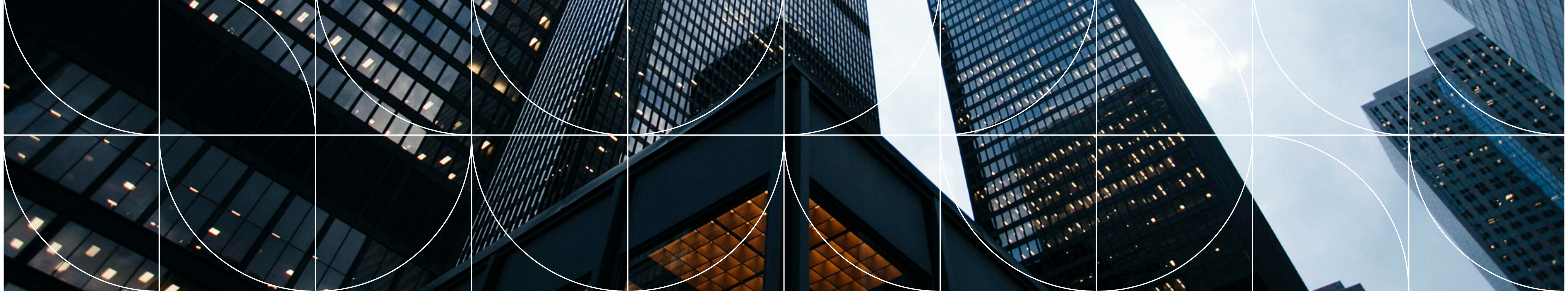
For another consecutive year, the health care industry can expect another record-breaking year of FCA enforcement. Through the end of September 2025, the US Department of Justice ("DOJ") already received $3.5 billion in FCA recoveries—$600 million more than the previous year's $2.9 billion in recoveries.

In June 2025, the DOJ further announced a record-breaking 2025 National Health Care Fraud Takedown involving over $14.6 billion in alleged fraud, more than doubling the prior annual record. Notably, this historic takedown resulted in criminal charges against 324 defendants, including 96 doctors, nurse practitioners, pharmacists, and other licensed medical professionals, in 50 federal districts and 12 State Attorneys General's Offices across the United States, for their alleged participation in various health care fraud schemes.

In May 2025, the DOJ also announced its first ever White-Collar Enforcement Plan with key points including: (1) health care violations remain top priorities for both criminal and civil enforcement; (2) whistleblower awards now cover reports involving public health care programs; and (3) the DOJ signals less reliance on corporate monitors—though oversight by Office of the Inspector General for the US Department of Health and Human Services and state regulators remains likely.

In July 2025, the DOJ and the Department of Health and Human Services ("HHS") also made a joint statement on the formation of a new False Claims Act Working Group to coordinate fraud and abuse actions. The working group is a cross-agency effort and includes the following entities: (1) HHS Office of General Counsel; (2) Centers for Medicare & Medicaid Services; (3) Center for Program Integrity; (4) Office of Counsel to the HHS Office of Inspector General, and (4) DOJ's Civil Division, with designees representing US attorneys' offices. As part of this announcement, DOJ leadership expressly identified traditional enforcement priorities, including Medicare Advantage, kickbacks, and drug and device pricing schemes, as continued targets of FCA action as well as emphasized a focus on less traditional priority areas, including network adequacy requirements, barriers to patient access to care, and use of electronic medical records systems to drive inappropriate utilization of care.

In short, FCA enforcement remains a top priority for the DOJ in 2026. Health care entities should continue to strengthen their compliance programs, prioritize internal reporting mechanisms, and prepare for more aggressive, coordinated enforcement that targets both traditional fraud schemes and emerging risk areas.



Key Trends in Commercial Litigation

Real Estate Litigation

— By Elizabeth Schrero and Mark Johnson

We expected that 2025 would usher in a general rebound in the real estate market after the rapid rise in interest rates the past several years, with a resulting increase in deal activity that would spawn litigation disputes, particularly in the warehouse and data center industries. That did not bear out last year.

The unpredictability of a global market and tariff uncertainties have shunted that growth. However, there are several areas in which we predict renewed focus, including landlord-tenant disputes, mortgage fraud arising from flip transactions of commercial real estate, and litigation-assisted, pre-suit demands, notices, workouts, surrender agreements, settlement agreements and other litigation-adjacent activity.

Commercial Landlord-Tenant Disputes

We have seen disputes arising from delay in complying with deadlines for alteration work and opening for business under lease agreements as well as guaranty litigation in the retail sector. We have also seen increasing pressure in the commercial retail space in 2025, which will force tenants and landlords to address ongoing tenancy issues with landlords hoping to maximize occupancy rates. This pressure will affect the retail sector as well, with tenants seeking to strictly enforce protections such as co-tenancy provisions and restrictive covenants.

Guaranty Litigation

Commercial landlords who gave rent concessions during the pandemic or extended leases on generous terms so as not to have a vacancy, now appear increasingly willing to draw the line and stand firm. One example of litigation on the rise is "Good Guy" guaranty-related disputes initiated by commercial owners who seek to reject a tenant's notice of intent to vacate premises early, in an attempt to avoid the guarantor's liability for rent which will accrue during the remaining lease term. Recent litigation has narrowed landlord protections under "Good Guy" guaranties, holding that a guarantor's liability ends when the tenant vacates and surrenders possession of premises even without a formal acceptance of surrender from the landlord, provided the conditions for surrender under the guaranty were satisfied. We expect more guaranty-related litigation going forward.

> We anticipate a greater number of bankruptcy filings by challenged borrowers and exposed guarantors, in 2026.

Increased Scrutiny of Flip Transactions

Over the past several years, an emerging trend has been the increase in same-day buy/sell real estate flip transactions. Under the typical pattern, an innocent seller of commercial property, frequently a multi-family property, enters into an arms-length transaction to sell to a buyer (Buyer A) which is a limited liability company comprised of a sole member. The sole member then sells 100% of its membership interest in Buyer A to Buyer B, an insider, which transaction is financed by a lender at a vastly inflated purchase price based on false financials submitted by Buyer A and Buyer B. In order to effectuate the scheme, both transactions are handled on the same day by the same title agent who issues a title policy on behalf of a title company. Typically, the initial arms-length transaction by owner to Buyer A occurs in the morning and the subsequent fraudulent membership interest sale by Buyer A to Buyer B occurs in the afternoon at a much inflated purchase price. The result is that the lender has over-extended itself, with the true value of the property being far less than the secured financing amount extended by lender to Buyer B. Buyer A then pockets the inflated purchase price to the detriment of the lender.

Lately, various private and public lenders have begun to re-examine these flip transactions, which have left them over-secured with the value of the underlying collateral being vastly over leveraged and leaving no actual equity or prospects to recover the outstanding debt. There have been several high-profile claims against not only insiders perpetrating such fraud but also the title companies whose agents handled both transactions and undoubtedly recognized the vast disparity in sale prices between the two same-day transactions. This heightened scrutiny is expected to pick up in 2026.

Foreclosure Litigation

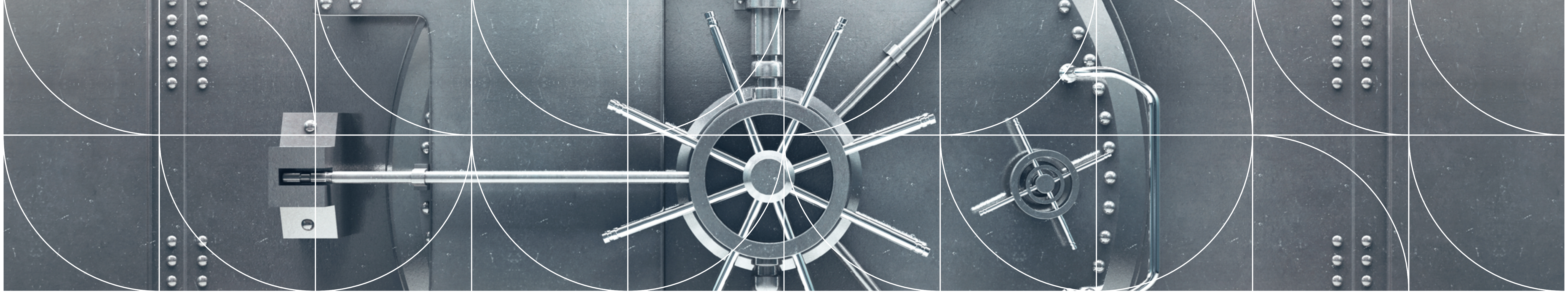
Lenders do appear less willing now to simply kick the can down the road with another maturity date extension, continued concession or deferral. We have seen higher numbers of defaults even on multi-family and mixed-use properties, with significant exposure to guarantors who are unable to extend or refinance loans. Foreclosure litigation, however, has not yet increased at a similar rate; rather, it appears many owners are not contesting and litigating, but are handing back the keys to their lenders. Dan Duarte, director of the special assets department at Tri-Counties Bank is quoted as saying about one-third of distressed borrowers are offering deeds-in-lieu to their lenders.

We anticipate a greater number of bankruptcy filings by challenged borrowers and exposed guarantors, in 2026.

> Data centers seem to be thriving widely, to satisfy demand from increased AI usage and e-commerce.

Sundry Real Estate Litigation Trends

The real estate landscape reflects uneven rebound across property types and locations. Real estate stress continues with persistently elevated though slightly lower interest rates, higher construction costs with tariffs and labor shortages, exacerbated by immigration enforcement, skyrocketing insurance costs (especially in areas at high risk of natural disasters), and the impact of climate change and natural disasters. Shifting concentrations of population and population growth, corporate relocations, as well as the Federal Government's closures and retrenchment, also has affected property asset types and regions differently across the country. As stated at a recent Seyfarth roundtable, like the general divide in the economy between the "haves" and "have nots", the real estate market is increasingly split between well-located, high-quality properties and properties needing updates or repositioning, with the former rebounding if not thriving, and the latter struggling or in foreclosure, bankruptcy or workout mode. The drop in office vacancy rates has been fueled by tenant interest in high-quality, class-A space. Data centers seem to be thriving widely, to satisfy demand from increased AI usage and e-commerce. Other trends include the urgent need for lower cost and affordable housing in some jurisdictions, as well as the rise of conversions of under-performing office properties to residential use, under new, relaxed governmental regulations and requirements.



Key Trends in Commercial Litigation

Trade Secrets, Computer Fraud & Non-Competes

— By Dawn Mertineit and Robyn Marsh

Restrictive covenant law experienced major shifts last year, and 2026 promises more scrutiny from the judiciary and legislators alike.

While the Federal Trade Commission ("FTC") withdrew its pursuit of a ban on non-competes, states continue to recalibrate their respective laws, impacting how businesses must draft their agreements. Accordingly, businesses seeking to protect their long-standing customer relationships and trade secrets must continue to navigate an ever-changing and challenging minefield to ensure that their restrictive covenants remain enforceable.

Federal Restrictions on Non-Competes

As anticipated, in 2025, the FTC voluntarily dismissed appeals to the Fifth and Eleventh Circuits, effectively walking away from its stalwart efforts to enforce a nationwide ban on most non-competes. Nonetheless, it has not completely abandoned its focus on non-competes. We anticipate focused crackdowns, especially with respect to specific career segments (e.g., health care providers), and heightened scrutiny on a case-by-case basis. Indeed, the FTC recently invited public input regarding "the scope, prevalence, and effects of employer non-compete agreements," to "inform possible future enforcement actions." Put simply: the regulatory pressure is far from disappearing.

We anticipate focused crackdowns, especially with respect to specific career segments (e.g., health care providers), and heightened scrutiny on a case-by-case basis.

State-Level and Judicial Initiatives

Notwithstanding the FTC's abandoned efforts to effectuate a nationwide ban, states continue to reshape regulation of restrictive covenants. Recent updates include industry-specific legislation limiting the scope of permissible covenants (most notably in the health care industry), and on the other end of the spectrum, the enactment of legislation in Florida to bolster its already pro-employer laws through the "CHOICE Act." This statute permits employers to (1) retain an employee during a lengthy, paid "notice period" where the employer can effectively sideline an employee from competitive employment while paying benefits and wages; and/or (2) implement certain non-competes for up to four years. This marks a significant turn in state law trends that typically afford *more* rights to employees. While we anticipate that states will largely continue to limit, rather than expand, restrictive covenant enforceability, other states may follow Florida's lead.

We also expect that courts may put a proverbial thumb on the scale of enforceability, making it harder for businesses to enforce restrictive covenants. For example, in Delaware, despite the well-established public policy favoring "freedom of contract," the Delaware Chancery Court continued its trend of sharply limiting enforcement of restrictive covenants, holding that a former employee's forfeited shares were insufficient consideration to support the enforcement of restrictive covenants. This holding signals tension with the Delaware Supreme Court's decision in 2024 holding that forfeiture-for-competition provisions in partnership agreements are enforceable and not subject to the "reasonableness" review typically applied to restrictive covenants. Indeed, the Delaware Supreme Court recently overturned the Chancery Court ruling regarding forfeiture, finding that the former employee's forfeited shares were not per se insufficient because they were cancelled; instead, the Delaware Supreme Court held that adequacy of consideration is determined at the time of execution, and remanded the case to the lower court.

We also expect that courts may put a proverbial thumb on the scale of enforceability, making it harder for businesses to enforce restrictive covenants.

In a similar vein, Massachusetts' highest court confirmed in 2025 that the state's 2018 non-compete statute—which includes strict requirements for non-compete enforcement—does not apply to non-solicits, even those accompanied by a forfeiture. On the other hand, a Massachusetts Superior Court recently interpreted the 2018 statute to permit non-competes in the employment context *only* if they are between the employee and the specific employer—foreclosing enforcement of covenants with a corporate parent (as is common in equity agreements).

In sum, it is more important than ever for employers to ensure their restrictive covenants are compliant with governing law and reasonably limited in scope to protect legitimate business interests to ensure enforceability.

Trade Secret Trends

Since restrictive covenants can be challenging to enforce, trade secret protection and related litigation will remain a top priority in 2026. Employers must have a clear action plan for both proactive and reactive efforts in the event of potential misappropriation. The wide availability of cloud-based transfer and storage technology, particularly for companies with a remote-employee base, can make it challenging to discern actual threats. Companies should have a belt-and-suspenders approach to ensure protection of critical trade secrets, because in the event of misappropriation, courts will deny relief to those who fail to demonstrate reasonable efforts to protect them.

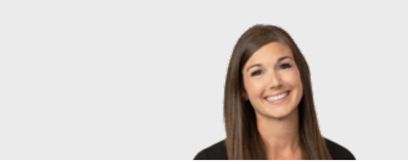
For example, in August 2025, the Tenth Circuit Court of Appeals held that a party that fails to take adequate steps to protect confidential information cannot maintain claims for trade secret misappropriation under *either* federal or state law. In stark contrast, in July 2025, a federal jury awarded an eye-popping verdict of nearly $29 million in actual damages and *an additional* $30 million in punitive damages after determining that the plaintiff's confidential information had been misappropriated in violation of confidentiality obligations and the company's existing protective measures. The juxtaposition of these outcomes highlights the need for ongoing vigilance to protect trade secrets through strong confidentiality practices, well-drafted contracts, and rigorous internal controls amid an ever-evolving technological landscape.

Companies should have a belt-and-suspenders approach to ensure protection of critical trade secrets, because in the event of misappropriation, courts will deny relief to those who fail to demonstrate reasonable efforts to protect them.

Conclusion

Businesses should regularly review their restrictive covenants agreements to ensure compliance with various state laws, federal rules, and/or judicial trends. They should also take measures to prevent information loss and mitigate harm that may occur notwithstanding best efforts to prevent trade secret misappropriation.

Authors



Kristine Argentine
Partner and National Chair, Consumer Class Action Defense Group
(312) 460-5332
kargentine@seyfarth.com

Teddie Arnold
Partner and National Co-Chair, False Claims, Whistleblower, and Internal Investigations Group
(202) 828-3597
earnold@seyfarth.com

Aaron Belzer
Partner, Commercial Litigation Practice Group
(310) 201-1546
abelzer@seyfarth.com

Jay Carle
Partner and Chair, Digital Asset & Technology Advocacy (DATA Law) Practice Group
(312) 460-6426
jcarle@seyfarth.com

Matthew Catalano
Partner, Securities and Fiduciary Duty Litigation Practice Group
(212) 218-5258
mcatalano@seyfarth.com

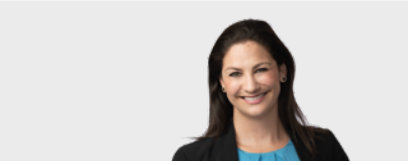
Matthew Christoff
Partner, Digital Asset & Technology Advocacy (DATA Law) Practice Group
(312) 460-5315
mcatalano@seyfarth.com

Jesse Coleman
Partner and National Co-Chair, Health Care Group
(713) 238-1805
jcoleman@seyfarth.com

Mark Johnson
Partner and National Co-Chair, Real Estate Litigation Practice Group
(312) 460-5627
majohnson@seyfarth.com

Yumna Khan
Associate, Commercial Litigation Practice Group
(713) 238-1835
ykhan@seyfarth.com

Lauren Leipold
Partner, Intellectual Property Practice Group
(404) 885-6737
lleipold@seyfarth.com



Robyn Marsh
Partner, Trade Secrets, Computer Fraud & Non-Competes Practice Group
(312) 460-5308
rmarsh@seyfarth.com

Dawn Mertineit
Partner and National Co-Chair, Trade Secrets, Computer Fraud & Non-Competes Practice Group and Co-Chair, Boston Litigation Department
(617) 946-4917
dmertineit@seyfarth.com

Matthew Moersfelder
Partner, Intellectual Property Practice Group
(206) 946-4931
mmoersfelder@seyfarth.com

Joe Orzano
Partner and National Co-Chair, Product Liability Practice Group and National Co-Chair, Advertising & Marketing Group
(617) 946-4952
jorzano@seyfarth.com

Will Prickett
Partner and National Co-Chair, Securities and Fiduciary Duty Litigation Practice Group
(617) 946-4902
wprickett@seyfarth.com

Jason Priebe
Partner, Associate General Counsel and Midwest Regional Manager, Privacy Compliance, Litigation & Cybersecurity
(404) 885-6773
jpriebe@seyfarth.com

Puya Partow-Navid
Partner, Intellectual Property Practice Group
(310) 201-1550
ppartownavid@seyfarth.com

Danny Riley
Associate, Digital Asset & Technology Advocacy (DATA Law) Practice Group
(312) 460-5310
driley@seyfarth.com

Christopher Robertson
Partner and National Co-Chair, False Claims, Whistleblower, and Internal Investigations Group
(617) 946-4989
crobertson@seyfarth.com

Sam Rowley
Partner, Commercial Litigation Practice Group
(617) 946-4851
srowley@seyfarth.com

Vincent Sama
Partner and National Co-Chair, Securities and Fiduciary Duty Litigation Practice Group
(212) 218-3368
vsama@seyfarth.com

Elizabeth Schrero
Partner and National Co-Chair, Real Estate Litigation Practice Group
(212) 218-5522
eschrero@seyfarth.com

John Skelton
Partner and National Chair, Franchise & Distribution Practice Group
(617) 946-4847
jskelton@seyfarth.com

James Sowka
Partner, Bankruptcy Litigation and Restructuring Group
(312) 460-5325
jsowka@seyfarth.com

Authors

Owen Wolfe
Partner, Intellectual Property Practice Group and National Co-Chair, Appellate Group
(312) 460-5657
swood@seyfarth.com

Shawn Wood
Partner and National Chair, Commercial Litigation Practice Group
(312) 460-5657
swood@seyfarth.com

Rebecca Woods
Partner and National Co-Chair, Commercial Litigation Practice Group and Chair, Atlanta Litigation Department
(404) 885-7996
rwoods@seyfarth.com

Paul Yovanic
Partner, Consumer Class Action Defense Group
(312) 460-5154
pyovanic@seyfarth.com

Seyfarth

"Seyfarth" and "Seyfarth Shaw" refer to Seyfarth Shaw LLP, an Illinois limited liability partnership. Our London office operates as Seyfarth Shaw (UK) LLP, an affiliate of Seyfarth Shaw LLP. Seyfarth Shaw (UK) LLP is a limited liability partnership established under the laws of the State of Delaware, USA, and is authorised and regulated by the Solicitors Regulation Authority with registered number 556927. Legal services provided by our Australian practice are provided by the Australian legal practitioner partners and employees of Seyfarth Shaw Australia, an Australian partnership. Seyfarth Shaw (賽法思律師事務所) is a separate partnership operating from Hong Kong as a firm of solicitors.

Prior results do not guarantee a similar outcome. #26-10045 M3

www.seyfarth.com