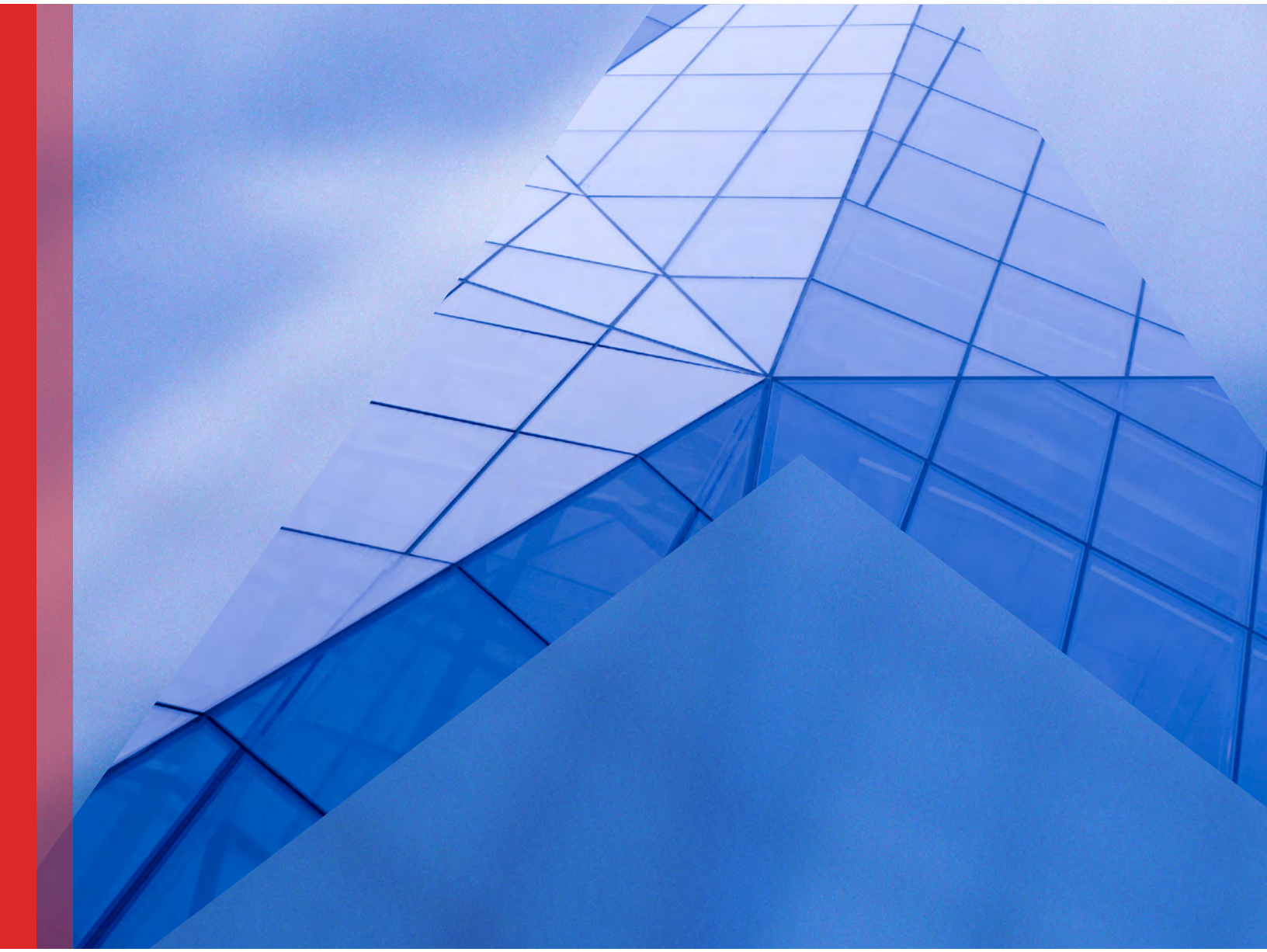
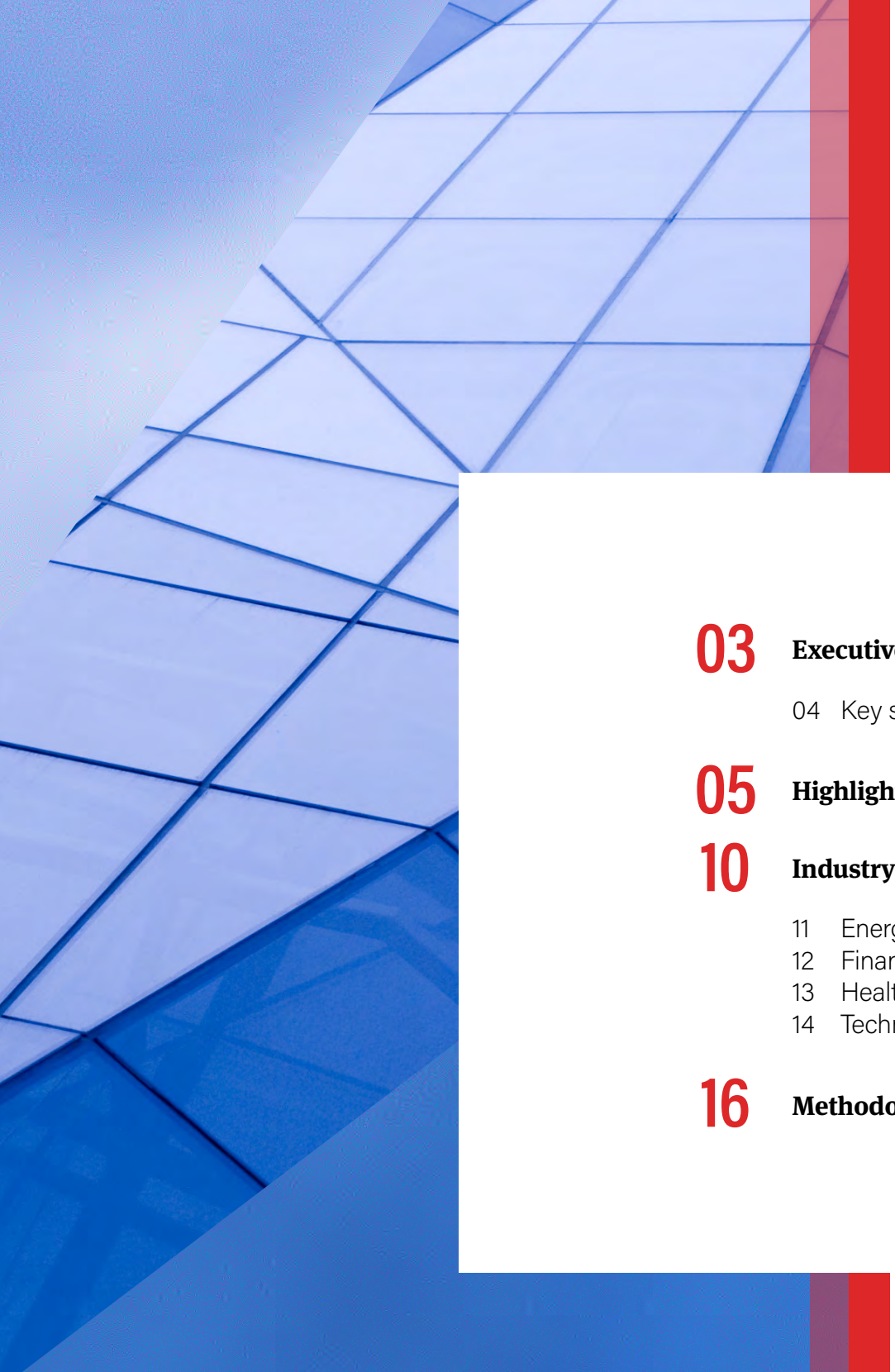
NORTON ROSE FULBRIGHT

2026 Annual Litigation Trends Survey

2026 Annual Litigation Trends Survey:

A midyear industry pulse





03 **Executive summary**

04 Key statistics

05 **Highlights of findings**

10 **Industry trends**

11 Energy
12 Financial institutions
13 Healthcare
14 Technology

16 **Methodology**

Executive summary

The US litigation landscape is evolving at a rapid pace in 2026, from AI market shocks to emerging class action risks. Corporate exposure to cybersecurity, data privacy, AI and employment disputes is deepening, while policy shifts and diverging federal-state enforcement priorities are adding to companies' compliance pressures.

To help corporate counsel navigate this unpredictable environment in real time, Norton Rose Fulbright conducted a midyear poll in March that focused on four key industries: energy, financial institutions, healthcare and technology. This targeted research draws on insights from 135 corporate counsel at US-based organizations across those four verticals, which accounted for 60% of the total respondent pool from our 2026 Annual Litigation Trends Survey.

This midyear pulse analyzes the latest results across all four industries to provide a topline view of how litigation risk is changing in what has already proven to be an eventful year. We also break out the results by industry to assess the impact those shifts are having on each sector.

> "The pace of change is striking, particularly in cyber breach-related actions and consumer products class actions; we're seeing activity and new approaches at a level not seen in years. Even where federal oversight has eased, states are often making up the difference, and that is pushing litigation forward across a broad range of areas.
>
> **Steven Jansma**
> Head of Litigation and Disputes, United States

Key statistics



Cybersecurity and data privacy is the leading area where dispute exposure has deepened since the start of 2026.

More than half of all respondents report increased federal- (56%) and state-level (53%) exposure, outpacing expectations outlined in our January 2026 research.

Technology respondents report the highest shares of increased federal and state-level exposure by industry – 75% and 72%, respectively.



Class action risk still centers on cybersecurity and employment issues.

Data or cybersecurity breaches (51%) are the leading events that all respondents consider likely to trigger class action litigation in 2026, followed by workforce changes such as layoffs or policy shifts (47%).

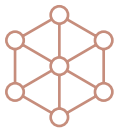
Product launches or AI-enabled deployments (41%) emerge as a likely catalyst, with healthcare respondents (53%) the most likely to cite it among industries.



AI litigation exposure is elevated as adoption advances.

Forty-six percent report more federal dispute exposure, and 42% cite state-level increases.

However, the AI-related litigation risk is distributed, with no single area cited by a majority of respondents and key risks varying by industry and organizational revenue.



Legal teams report broad improvements on cost pressures since late 2025.

Fifty-five percent cite improvements in managing internal legal budgets, and for 71% of respondents, managing outside counsel costs has become easier or remained the same, offering a more optimistic picture on legal spend than many anticipated entering 2026.

Technology and energy respondents are more likely to cite litigation readiness improvements.

Highlights of findings

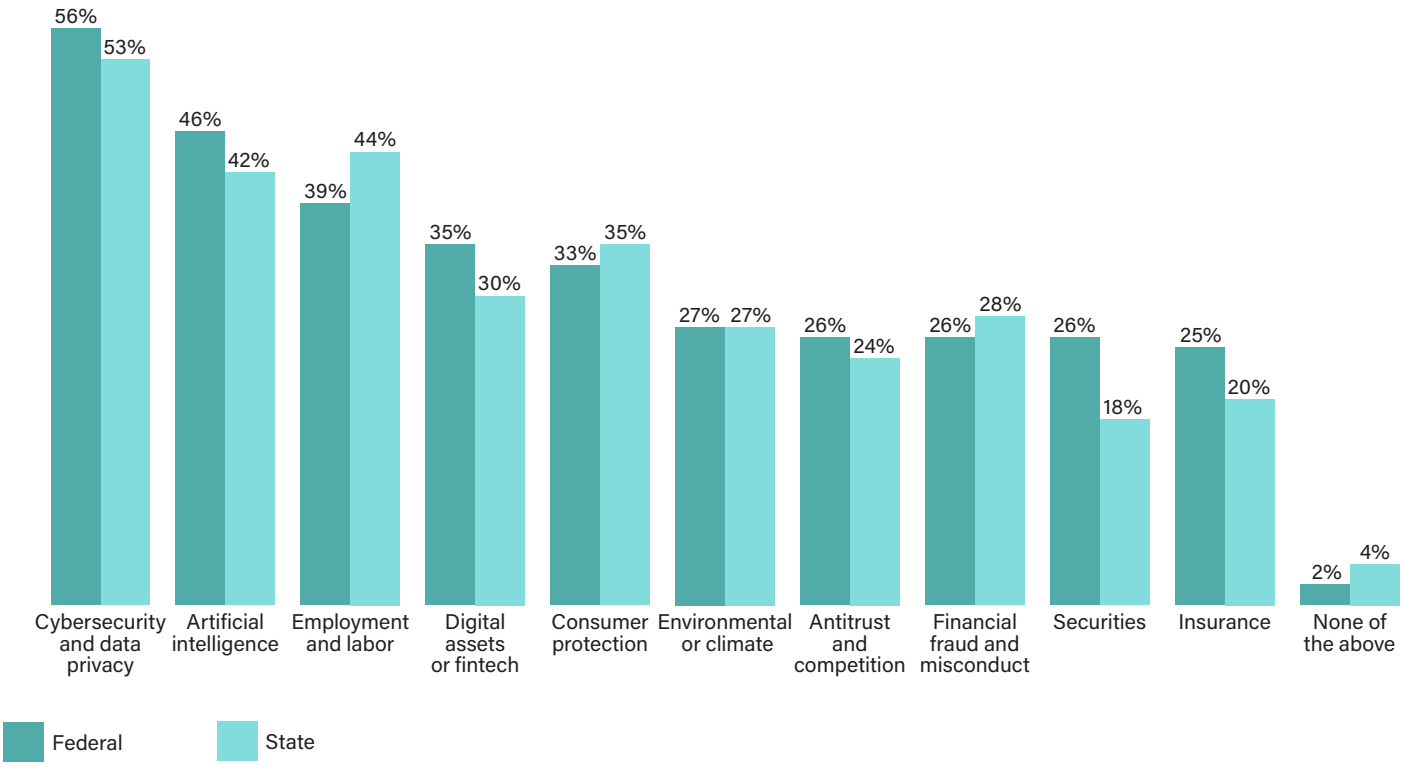
Dispute risk hotspots: Cybersecurity, AI and employment

Cybersecurity and data privacy has emerged as the leading area of increased dispute exposure across the four key industries since the start of 2026, and the magnitude of that risk has far outpaced what corporate counsel anticipated. In late 2025, just 29% of energy, financial institutions, healthcare and technology respondents in our annual survey expected to face greater cybersecurity and data privacy exposure in 2026. Midyear, exposure appears to be increasing: 56% now report increased risk at the federal level and 53% at the state level.

Several factors may be driving this heightened level of midyear exposure. Emerging technologies including AI are accelerating the volume and sophistication of cyberattacks. Geopolitical conflicts further intensified the spotlight on such incursions and prompted multiple federal cybersecurity advisories warning about cyber actors targeting critical US infrastructure. "Cybersecurity risk was already high when this year began, and the 2026 data shows how rapidly exposure can multiply from there, as new technologies and geopolitical pressures converge," said Norton Rose Fulbright partner Ji Won Kim.

> "The responses confirm what we see in practice: enforcement risk has not receded, it has relocated. With 56% of counsel reporting more federal cyber exposure and 53% seeing the same at the state level, companies can now expect to be defending parallel investigations on two tracks – and state AGs are increasingly the more aggressive plaintiff in the room.
>
> **Andrey Spektor**
> Co-Head of Litigation and Disputes, New York

Federal versus state: Increase in dispute exposure



Q. Since the start of 2026, in which of the following areas has your organization's federal-level dispute exposure increased? Select all that apply.
Q. Since the start of 2026, in which of the following areas has your organization's state-level dispute exposure increased? Select all that apply.

More generally, perpetually evolving cybersecurity and data privacy requirements continue to expose companies to multijurisdictional enforcement, as does accelerating AI use across organizations.

Respondents also report increased litigation risk around AI since the start of this year, suggesting that earlier concern about the technology's risks – in our annual report, 59% of all respondents said managing litigation risk surrounding AI was a challenge – is now materializing as actual exposure. Forty-six percent of all respondents report more federal dispute exposure, and 42% cite state-level increases.

Employment and labor risk continues to be a major issue for companies, with 39% of all respondents citing increased federal dispute exposure and 44% reporting more at the state level. This reflects decentralized enforcement and increased compliance complexity as California, New York and other states pass new employment-related requirements.

> State-level employment exposure is rising as plaintiffs look to jurisdictions they view as more favorable, especially as federal interpretations shift. For multistate employers, that dynamic increases compliance complexity and forum risk in a very real way.
>
> **Kimberly Cheeseman**
> Co-Head of Litigation and Disputes, Houston

Fragmented AI risk landscape

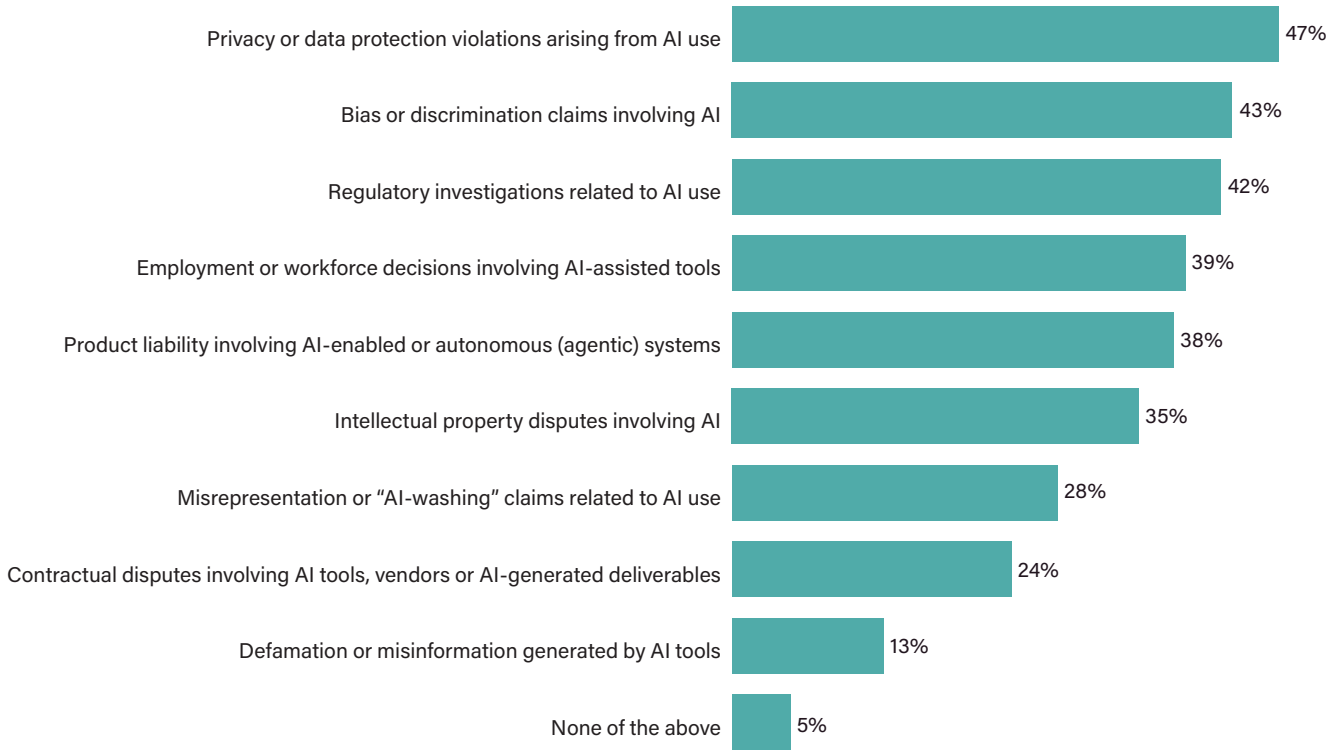
However, the AI-related litigation risk environment is distributed, with no single area cited by a majority of respondents, perhaps because AI presents overlapping legal issues that depend on how and where organizations deploy it. Forty-seven percent expect privacy or data protection violations arising from AI use to increase their litigation exposure between now and the end of 2026. Other leading risk areas include bias or discrimination claims involving AI (43%), regulatory investigations related to AI use (42%) and employment or workforce decisions involving AI-assisted tools (39%).

Importantly, AI-related litigation risk areas vary both by industry (see the sector breakout below) and by revenue level. Lower-revenue organizations (those with less than US$100 million in annual revenue) are more likely to cite AI-related privacy (53%), bias (47%) and IP (47%) risks. "Where AI is most clearly driving IP disputes is copyright, both around training data and outputs. We're also seeing trademark issues emerge around AI-generated images and logos," said Norton Rose Fulbright partner Stephanie DeBrow.

However, respondents with more than US$1 billion in revenue more frequently identify regulatory scrutiny (49%) and employment or workforce decisions (41%) as AI-related litigation risks.

> "AI and other emerging technologies are shedding new light on existing legal problems and intensifying the associated risks. The speed at which threats evolve is now outpacing how organizations can realistically adjust.
>
> **Ji Won Kim**
> Partner

AI-related risks contributing to increased exposure



Q. Between now and the end of 2026, which of the following AI-related risks do you expect to increase your organization's litigation exposure? Select all that apply.

Class action triggers

Class action risk across the four industries we surveyed remains anchored in cybersecurity and workforce issues. Asked which events they consider likely to trigger class action litigation against their organization this year, more than half (51%) of all respondents cite data or cybersecurity breaches while 47% cite workforce changes such as layoffs – both consistent with annual survey results.

AI tools appear to be an emerging class action catalyst, with 41% of all respondents identifying product launches or AI-related deployments as a likely trigger.

> Data breaches create uniquely high-stakes litigation because even 'small' incidents can trigger massive potential exposure to class actions once statutory damages and multistate laws come into play.
>
> **Edward Casmere**
> Co-Head of Litigation and Disputes, Chicago

Likely triggers of class action litigation through end of 2026



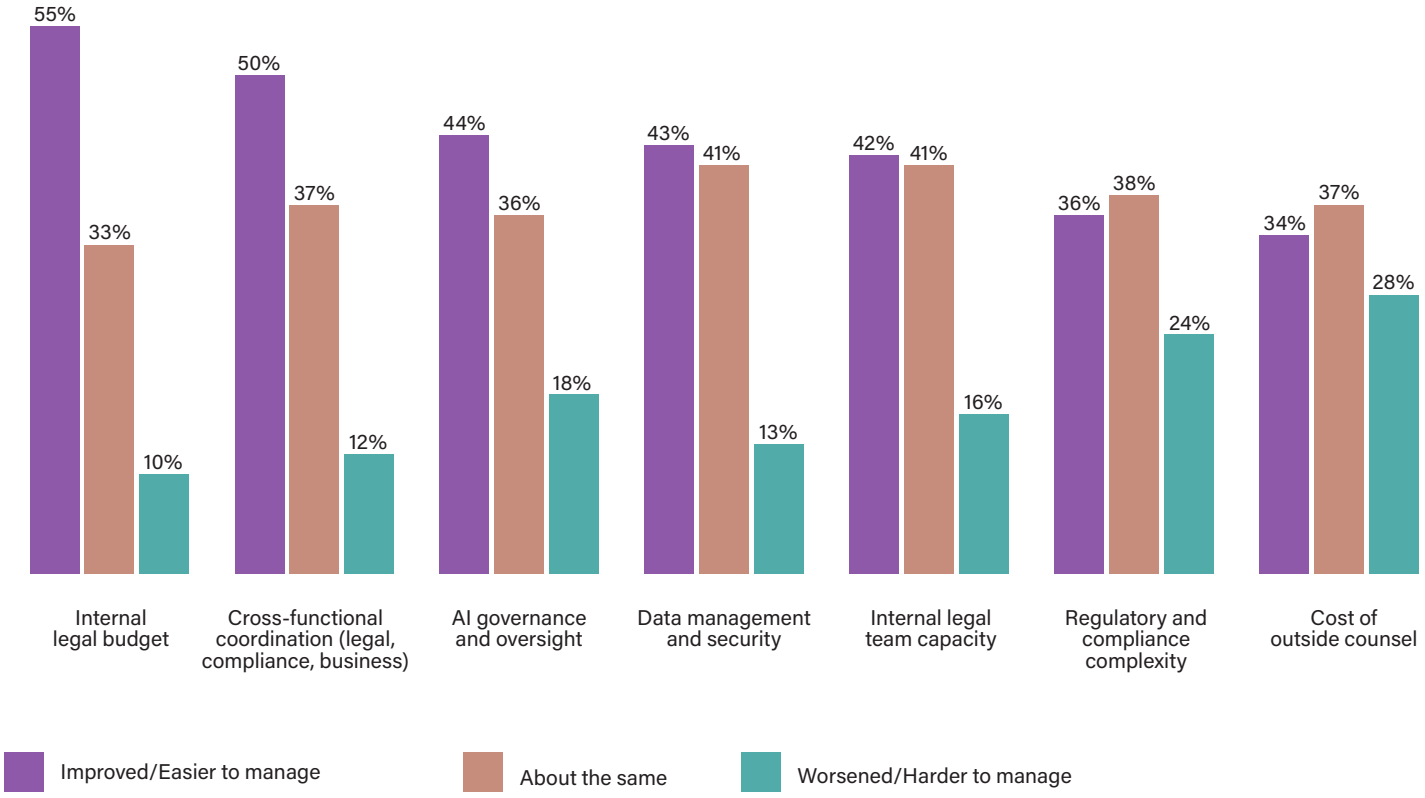
Q. Between now and the end of 2026, which of the following events do you consider likely triggers of class action litigation against your organization? Select all that apply.

Progress on litigation readiness

In-house legal teams report meaningful progress on internal constraints and challenges since late 2025, with some stabilization even on areas outside their direct control. Fifty-five percent say management of internal legal budgets has improved and half say the same of cross-functional coordination. On outside counsel costs, 71% say managing those costs has remained the same or become easier, even as regulatory and compliance complexity continues to be a challenge for the majority.

Lower-revenue organizations report the most improvements in data management (63%) and internal legal budgets (60%). AI governance has also improved for both lower- and higher-revenue respondents (50% each), in contrast to middle-revenue organizations, where only a third (33%) report progress.

LItigation risk preparedness since year-end 2025



Q. In late 2025, many legal teams reported feeling underprepared to manage litigation risk. Based on your experience, how have the following conditions changed since that time? ("Unsure" selections not shown on chart)

Industry trends

Top areas of increased dispute exposure by industry

	Rank	Federal	%	Rank	State	%
Energy	**T1**	Cybersecurity and data privacy	57%	**1**	Cybersecurity and data privacy	60%
	T1	Employment and labor	57%	**2**	Employment and labor	51%
	3	Environmental or climate	46%	**3**	Artificial intelligence	46%
Financial institutions	**T1**	Cybersecurity and data privacy	53%	**T1**	Employment and labor	44%
	T1	Consumer protection	53%	**T1**	Artificial intelligence	44%
	3	Artificial intelligence	47%	**3**	Cybersecurity and data privacy	41%
Healthcare	**1**	Artificial intelligence	53%	**1**	Employment and labor	50%
	2	Digital assets or FinTech	47%	**2**	Environmental or climate	44%
	3	Cybersecurity and data privacy	41%	**3**	Digital assets or FinTech	41%
Technology	**1**	Cybersecurity and data privacy	75%	**1**	Cybersecurity and data privacy	72%
	2	Artificial intelligence	50%	**2**	Artificial intelligence	53%
	3	Intellectual property	44%	**3**	Financial fraud and misconduct	41%

Q. Since the start of 2026, in which of the following areas has your organization's federal-level dispute exposure increased? Select all that apply.
Q. Since the start of 2026, in which of the following areas has your organization's state-level dispute exposure increased? Select all that apply.

Energy

Employment litigation is top of mind for energy respondents. They are the most likely (57%) of any industry to consider workforce changes a likely class action trigger in 2026, compared to less than 45% in the other three industry groups we surveyed (44% in financial institutions, 44% in technology and 41% in healthcare). Energy respondents also report the highest share of increased employment and labor dispute exposure across industries at both the federal (57%) and state (51%) levels.

This could be due to structural factors, with energy prone to cyclical workforce volatility tied to commodity prices. The industry also relies in part on hourly workers and contractors, which can increase vulnerability to claims around wage and hour compliance, working conditions, overtime and employee classification.

Cybersecurity and data privacy tied with employment and labor as the top-ranked area of increased federal-level dispute exposure for energy respondents (57%) – and it was their leading risk area at the state level (60%). Environmental or climate exposure also remains a factor at the federal level (46%). "In the energy sector, some ESG-related litigation pressures appear to be easing, but disclosure decisions still carry significant disputes risk," said Norton Rose Fulbright partner Rachel Roosth.

On the upside, energy respondents are more likely to cite gains in litigation readiness since late 2025. Sixty percent say cross-functional coordination across legal, compliance and business groups has improved, and 54% report progress in AI governance and oversight – more than those in any other industry.

> "In litigation-heavy industries like energy, cross-functional coordination tends to reflect experience. Teams that live with constant disputes build systems to respond quickly, but anticipating the next risk before it arrives remains the challenge.
>
> **Andrew Price**
> Co-Head Commercial and Energy Disputes, United States

Financial institutions

Financial institution respondents report the lowest share of increased dispute exposure among industries at both the federal and state levels, with an average of 28% selecting each category across both jurisdictions.

That said, more than half report increased federal exposure to cybersecurity and data privacy (53%) and consumer protection disputes (53%), which represent the top-ranked areas for the industry, followed by AI (47%). Data breaches or cybersecurity incidents are also this group's most-cited likely class action trigger for 2026 (56%).

Together, these results reflect the industry's digital maturity – and larger attack surface – with banks and FinTech companies housing troves of sensitive personal and financial data. Given the industry's high degree of federal oversight, corporate counsel may be concerned that private litigation activity tied to federal rules will increase even as agency-level enforcement in some areas eases under the current administration.

At the state level, employment and labor (44%) and AI (44%) are the top-ranked areas where financial institutions respondents cite increased dispute exposure since the start of this year. This aligns with findings from our annual survey about stepped-up state-level enforcement, as well as ongoing state efforts to regulate AI. Financial institutions also have relatively advanced AI deployments, and product liability involving AI-enabled or autonomous (agentic) systems is the leading area where industry respondents anticipate AI-related litigation risk.

> "Consumer protection and cybersecurity exposure remain the day-to-day reality for financial institutions. What's newer is how even a relatively modest data leak can snowball into a wave of class actions, including when the breach starts with a vendor rather than the bank itself.

Steve Dollar
Co-Head of Financial Institutions Disputes, United States

Healthcare

Overall, healthcare respondents report the highest share of increased litigation exposure at both the federal and state levels, with an average of about 35% selecting each category for both jurisdictions. That makes sense given the persistent litigation readiness challenges healthcare respondents report. Thirty-five percent say regulatory compliance complexity has increased since late 2025, while 32% say internal legal team capacity has decreased.

Healthcare's growing deployment of AI across operational and clinical functions is increasing litigation risk on multiple fronts. Fifty-three percent of respondents say AI exposure has increased at the federal level. The same share consider AI-enabled product deployments and product launches a likely trigger of class action litigation – it is the leading such catalyst for healthcare and the highest percentage by industry. Healthcare respondents are also the most likely to say that issues around AI governance and oversight have heightened (26%) since late 2025, with only 29% reporting improvement in that area.

At the state level, employment and labor (50%) is the top-ranked area of increased dispute exposure, with labor shortages, use of contract labor and wage-and-hour complexity likely factors. However, only 26% cite increased state-level AI dispute exposure, making healthcare an industry outlier.

> "For healthcare, the first AI question is whether the system is truly closed. If patient information can escape the perimeter, the issue quickly becomes a HIPAA problem.
>
> **Jay Dewald**
> Head of Healthcare Investigations, United States; Head of Litigation and Disputes, San Antonio

Technology

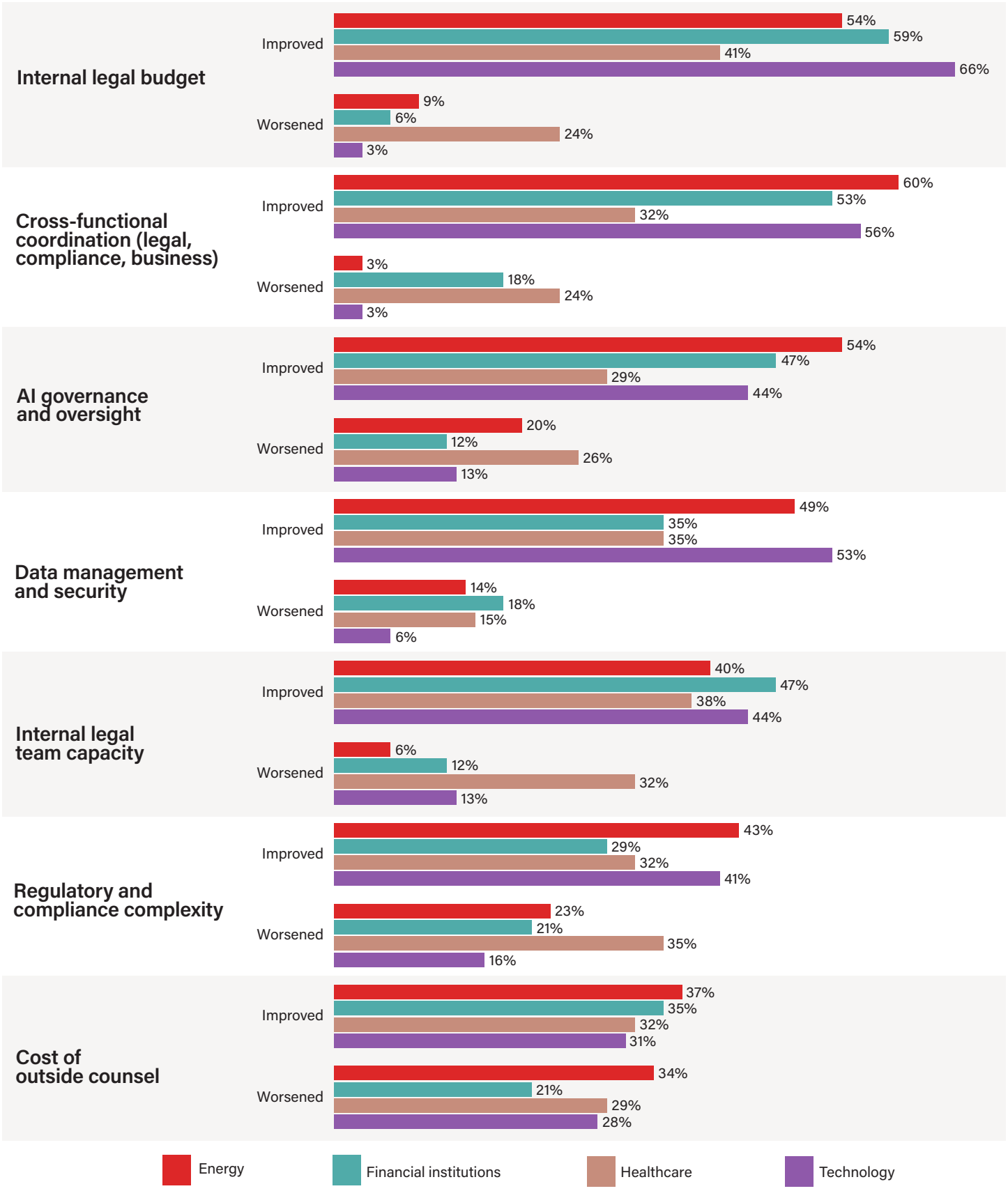
Roughly three quarters of technology respondents say cybersecurity and data privacy dispute exposure has increased since the start of 2026 at both the federal (75%) and state (72%) levels – the highest share by industry. That may reflect the dual vulnerabilities for technology companies, which are both targets for cyberattacks and providers of digital infrastructure that may be liable in the event of attacks on their customers. Relatedly, data breaches are the most likely class action trigger for technology respondents (69%).

AI dispute exposure also increased at the federal (50%) and state (53%) levels, with 47% of technology respondents citing product launches or AI-enabled product deployments as a likely class action trigger. When it comes to AI-related risks, 56% expect privacy or data protection violations arising from AI use to contribute to their organization's litigation exposure, with half citing bias or discrimination claims and intellectual property disputes involving AI.

Technology respondents were more likely than other industries to report progress on internal legal budgets (66%) and data management and security (53%) since the start of 2025, suggesting efforts to address the above vulnerabilities.

> "AI-assisted hiring tools are creating real uncertainty for employers, particularly around bias and discrimination claims. The risk isn't theoretical – it's already being tested in courts and before the EEOC.
>
> **Kimberly Cheeseman**
> Co-Head of Litigation and Disputes, Houston

Litigation risk preparedness since year-end 2025: Industry comparisons



Q. In late 2025, many legal teams reported feeling underprepared to manage litigation risk. Based on your experience, how have the following conditions changed since that time? ("About the same" and "Unsure" responses not shown on chart)

Methodology

Norton Rose Fulbright conducted a midyear quantitative industry pulse survey to assess how litigation risk and enforcement dynamics are evolving in 2026.

The survey was fielded in March 2026, with 135 respondents participating across four key industries: energy, financial institutions, healthcare and technology. All respondents are in-house counsel at organizations based in the United States.

The targeted survey was designed to capture perspectives on emerging developments, including shifts in dispute exposure at the federal and state levels, triggers for class action litigation and the growing role of artificial intelligence in shaping litigation risk.

Contacts



Steven Jansma
Head of Litigation and Disputes, United States
San Antonio | Houston
+1 210 270 9366
steven.jansma@nortonrosefulbright.com



Ji Won Kim
Partner
Los Angeles
+1 213 892 9216
jiwon.kim@nortonrosefulbright.com



Edward Casmere
Co-Head of Litigation and Disputes, Chicago
Chicago | New York | St. Louis
+1 312 964 7778
ed.casmere@nortonrosefulbright.com



Rachel Roosth
Partner
Houston
+1 713 651 3734
rachel.roosth@nortonrosefulbright.com



Kimberly Cheeseman
Co-Head of Litigation and Disputes, Houston
Houston
+1 713 651 5160
kimberly.cheeseman@nortonrosefulbright.com



Andrey Spektor
Co-Head of Litigation and Disputes, New York
New York
+1 212 318 3130
andrey.spektor@nortonrosefulbright.com



Stephanie DeBrow
Partner
New York
+1 512 536 3094
stephanie.debrow@nortonrosefulbright.com

NT Analyzer

Evidence-based privacy risk assessments for digital properties

NT Analyzer is Norton Rose Fulbright's proprietary privacy forensics tool suite. It enables our Global Cybersecurity and Privacy team to capture and evaluate network traffic and runtime behavior of websites, mobile device applications and embedded systems such as medical devices and IoT services. Leveraging NT Analyzer, we can generate privileged privacy risk assessments based on objective facts, not assumptions or guesswork, that isolate root cause and enable practical mitigations.

We provide reports and actionable remediation items across a broad range of technical compliance benchmarks under various laws including CIPA, HIPAA, VPPA, GLBA, ECPA, CCPA (and other state privacy laws) and GDPR. Using NT Analyzer, we can also provide technical support and documentation for Data Protection Impact Assessments (DPIAs). We identify the technical issues through NT Analyzer, translate them into legal risks and provide clear, practical remediation guidance.

Hidden data collection and runtime behavior

Companies rely heavily on third parties for analytics, marketing, targeted advertising, location services and many other features embedded in digital properties. These third parties cause silent, hard-to-detect compliance failures (such as data leakage and non-working opt-outs). Our assessments and analyses are all conducted under attorney-client privilege.

Detection of transmitted data

NT Analyzer detects a broad range of transmitted data, including:
Traditional forms of directly identifiable data, hashed and encoded data
Unique IDs, including ad IDs, hardware IDs and network names
Geolocation information, such as latitude and longitude
Cookies and HTML5 local storage

What we do

Using NT Analyzer, we help clients answer the questions that matter most:
Why and how was data shared?
Did the cookie banner work?
Did the opt-out fail?
What code caused the issue?
What is the legal risk?
What are the potential fixes?

We empower organizations to take control of their digital privacy footprint. By uncovering hidden data flows, silent compliance failures and unwanted third parties, we enable proactive risk management grounded in objective evidence.

Contacts



Steven Roosa
Head of NRF Digital Analytics and Technology Assessment Platform, United States
+1 212 318 3222
steven.roosa@nortonrosefulbright.com



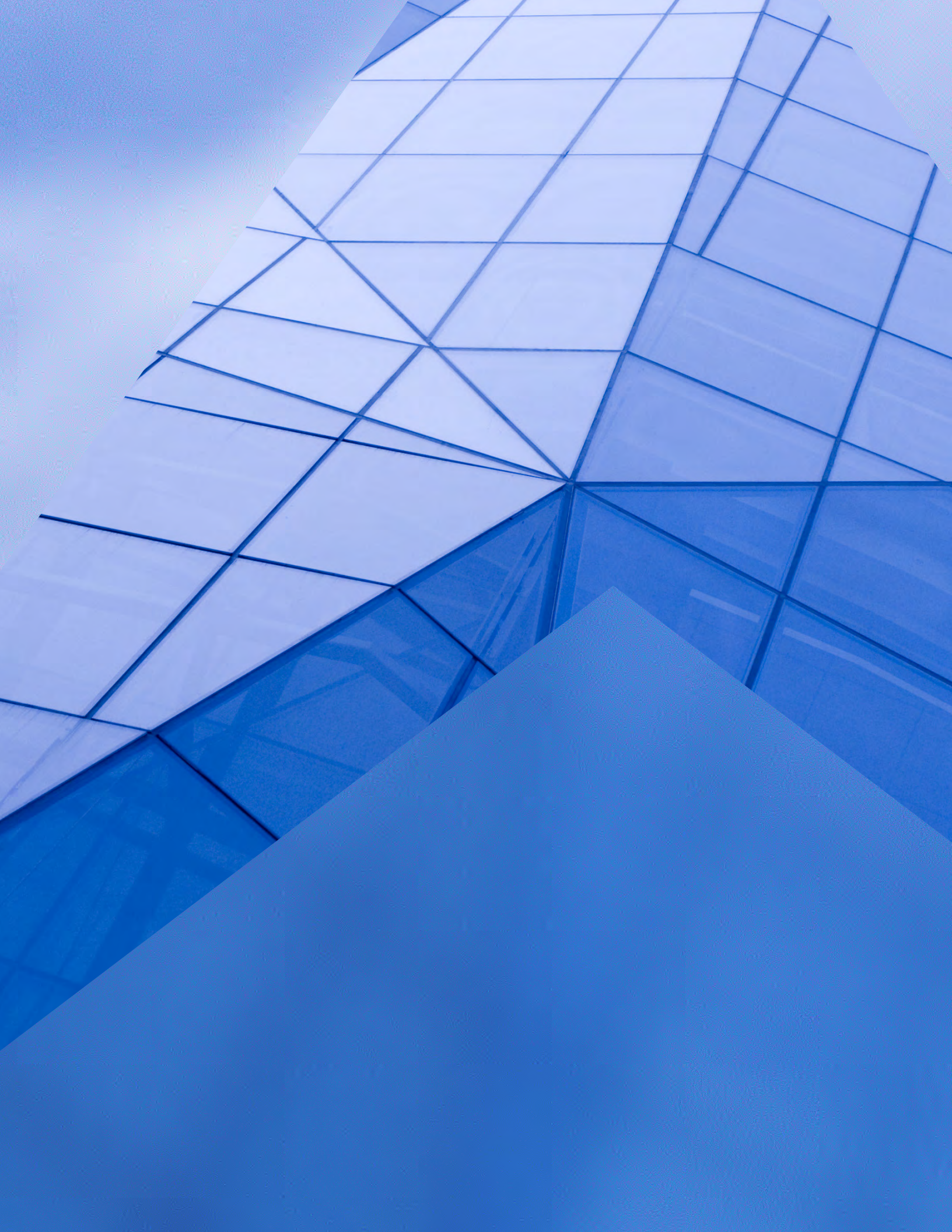
Wenda Tang
Senior Associate
+1 202 662 4536
wenda.tang@nortonrosefulbright.com



Shaun Abraham
Counsel
+1 713 651 2152
shaun.abraham@nortonrosefulbright.com



Kelly Atherton
Counsel
+1 612 321 2218
kelly.atherton@nortonrosefulbright.com



NORTON ROSE FULBRIGHT

Norton Rose Fulbright provides a full scope of legal services to the world's preeminent corporations and financial institutions. The global law firm has more than 3,000 lawyers advising clients across locations in the United States, Europe, Canada, Latin America, Asia, Australia, Africa and the Middle East.

nortonrosefulbright.com

The purpose of this communication is to provide information as to developments in the law. It does not contain a full analysis of the law nor does it constitute an opinion of any Norton Rose Fulbright entity on the points of law discussed. You must take specific legal advice on any particular matter which concerns you. If you require any advice or further information, please speak to your usual contact at Norton Rose Fulbright.

Norton Rose Fulbright © 2026. All Rights Reserved
US_70733 - 06/26